UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
PROGRAMA DE POSGRADO EN DERECHO
FACULTAD DE DERECHO

RÉGIMEN JURÍDICO DE LA TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL, DATOS PERSONALES Y BIG DATA

TESIS
QUE PARA OPTAR POR EL GRADO DE:
MAESTRO EN DERECHO

PRESENTA:
RAÚL TORRES JIMÉNEZ

TUTORA
DRA. MARÍA GUADALUPE FERNÁNDEZ RUÍZ
PROGRAMA DE POSGRADO EN DERECHO

CIUDAD UNIVERSITARIA, CD. MX, DICIEMBRE, 2022

Agradecimientos

A *ABBA* porque es el padre de todo. NSL.

A mis amorosos abuelos Ada y Miguel.

A mi madre Ada María, por todo el apoyo, amor y regaños.

A mi padre Joaquín, quien, desde el cielo, vela por su hijo.

A mi querida tutora y mentora, la Dra. Guadalupe Fernández, quien jamás dejó de creer y apoyarme.

A mi amada Lorena, por impulsarme, apoyarme, quererme, tolerarme, y sacar la mejor versión de mí.

A mi primo Jesús y mi hermano Samuel, por acompañarme siempre.

A mis tías y tíos, Clara, Jesús, Francisco y Raúl.

A mis amigos y hermanos de camino, Jorge Rojas, Javier Nava, Daniel Olguín, Rosalinda Pizarro, Rosa María Jiménez, Carmen López, Rafael Cabrera, Leonardo Alcántara, Carolina Zayas, Miriam Morán, Manuel León, Elizabeth Albarrán, Albert Baixés.

A mi club “ultra-ultra”, Sergio Guzmán y Leticia Isgleas (hasta España)

A mis doctores Carmen Domínguez y Mario por cuidar de mi salud.

A mi gran maestro José Antonio Ferrara, por iniciarme en el sendero del monje guerrero.

A mi *Shihan* Tohru Hayashi, por su enseñanza en el arte del Nippon Kempo.

A mi editora Beatriz Canales, por su apoyo en publicar mis artículos en Revista Consultoria.

A las Instituciones que me han formado y forjado en mi camino personal y profesional: UNAM, Facultad de Derecho, Federación Mexicana de Nippon Kempo, A.C., Cámara Nacional de Comercio Servicios y Turismo de la CDMX, Pentathlón Deportivo Militarizado Universitario.

Siglas

AEPD. Agencia Española de Protección de Datos. (España)

AGN. Archivo General de la Nación.

APEC. Foro de Cooperación Económica Asia-Pacífico.

CEPAL. Comisión Económica para América Latina y el Caribe.

IFAI. Instituto Federal de Acceso a la Información Pública, posteriormente llamado Instituto Federal de Acceso a la Información y Protección de Datos; después cambió a INAI.

IFT. Instituto Federal de Telecomunicaciones.

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

INEGI. Instituto Nacional de Estadística y Geografía.

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.

LGA. Ley General de Archivos

LGTAIP. Ley General de Transparencia y Acceso a la Información Pública

OCDE. Organización para la Cooperación y el Desarrollo Económicos

RGPD. Reglamento General de Protección de Datos. (de Europa)

RLFPDPPP. Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

UNESCO. Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura.

RÉGIMEN JURÍDICO DE LA TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL, DATOS PERSONALES Y BIG DATA

ÍNDICE

Introducción

Hoy en día la cantidad de datos que se mueve en el mundo es tal que las cifras cada vez más se vuelven inútiles en comparación con todo lo que se puede encontrar en la red de redes.

Los gobiernos hacen esfuerzos para regular los derechos que tienen las personas en acceder a todo tipo de información y a la vez a proteger los datos personales que cada vez se vuelven vulnerables por pate de personas y corporaciones que los emplean para diferentes fines. De igual forma, la ciberseguridad cada vez tiene varios problemas en cuanto a la manera en generar protocolos que cuiden el acceso a los datos de las personas y corporaciones y por otro lado los hackers que eventualmente acceden sin consentimiento a la vida privada de las personas.

Asimismo, el uso legítimo de los datos genera información útil para la vida cotidiana de las personas. Hacer un plan de negocios por ejemplo resulta cada vez más fácil si sabemos usar los datos que se generan constante mente en nuestro alrededor, provocando que podamos genera un diagnóstico más certero, tanto del tipo, como del lugar en dónde ubicar un negocio.

Por otro lado, los gobiernos han entendido la importancia de tener a la ciudadanía debidamente informada, lo cual ha quedado contemplado en los convenios Internacionales quienes han elevado la categoría del acceso a la información como un Derecho Humano, el cual solamente puede ser restringido por causas de interés público.

México es un país donde entramos tarde en las cuestiones de transparencia, acceso a la información y protección de datos personales. Hay que recordar que, apenas entrando el milenio, en 2002 se generó la primera Ley de Transparencia y Acceso a la Información durante la presidencia de Vicente Fox, posteriormente se crearía un órgano garante de este derecho que en un primer momento fue el IFAI que, por cierto, ha sido un organismo que en su devenir a cambiando de nombres y de naturaleza jurídica.

Adicionalmente, el acceso a la información ha sido vinculado también con la

rendición de cuentas, pero también con la protección de datos personales, que en este último caso tienen un doble carácter de protección. Por un lado, la protección de datos personales que detentan organismos públicos, y por otra parte los datos personales que son tratados por particulares. Es así que, a nivel federal la protección de datos personales en posesión de entes públicos solo había sido contemplada en la Ley Federal de Acceso a la Información hoy abrogada, pero no fue, sino que hasta el 2017 cuando se publicó una ley general que garantizó la protección *ex profeso*, de estos datos en posesión de sujetos obligados.

Por otro lado, la protección de datos personales en posesión de particulares también es un acontecimiento novedoso pues no ha sido, sino hasta el 2010 cuando se emite la primera y única ley con que contamos, donde bajo el mandato del entonces presidente Calderón se contempla que también los particulares son responsables de vigilar el tratamiento de Datos Personales, cuidando con ello el uso, manejo, aprovechamiento y obtención de los mismos.

El reto es grande, las reformas constitucionales en la materia van a cuentagotas y estamos en plena era de la información donde nuestro país va rezagado con respecto a Europa donde se tienen esquemas robustos en relación con el acceso a la Información y la misma protección de datos personales.

Veremos que nos deparan los siguientes años en la medida en que también se generen nuevos estudios como el que a continuación se presenta con el fin de ir fortaleciendo, sobre todo, la aplicación y protección de estos derechos.

Hipótesis, Variables, Dimensiones e Indicadores

El acceso a la información, los datos personales y el *big data*, tienen regulaciones específicas que permiten que las personas ejerzan sus derechos de manera amplia, así como tomar decisiones en los ámbitos público y privado.

Variables	Dimensiones	Indicadores
Datos Personales	Sujetos Obligados	Generales
		Particulares
		Orden Federal
		Orden Estatal
	En Posesión de Particulares	Tipos
		Consentimiento
		Derechos ARCO
Acceso a la Información	Obligaciones de Transparencia	Comunes
		Específicas
		Sistema Nacional de Transparencia
		Transparencia Proactiva
	Procedimientos	Acceso
		Clasificación
		Medios de Impugnación
		Medidas de Apremio
Big Data	Datos Abiertos	Gobierno Abierto
	Minería de Datos	Analítica de Datos

Objetivos

Objetivo General

Analizar las diferentes regulaciones con las que cuenta el acceso a la información, los datos personales y el *big data*.

Objetivos Específicos

1) Identificar, analizar y comparar la normatividad con la que cuenta el derecho de acceso a la información, en el ámbito nacional y en países como Estados Unidos, España y Argentina.[1]
2) Identificar, analizar y comparar la normatividad con la que cuenta el derecho de la protección de datos personales tanto por lo que hace a los sujetos obligados, como por lo que hace a los particulares.
3) Identificar y analizar el poder que tiene el *big data* en gobiernos y organizaciones para tomar decisiones.
4) Analizar las amenazas a la ciberseguridad con las que se pueden enfrentar tanto los gobiernos como los particulares estudiando figuras concretas como el *hackeo* o la suplantación de identidad entre otras.
5) Proponer formas de uso de la información y de las tecnologías de la información. por parte de los particulares.
6) Proponer formas en la que los particulares pueden cuidar la seguridad de los datos que reciban tratamiento.

[1] Se toman estos países porque es dónde se ha desarrollado más la doctrina y la legislación en la materia de investigación.

Metodología de la Investigación

Obtención de la Información

Directa: Documentos de clientes personales tanto por lo que hace al cumplimiento de la obligación de sujetos obligados como por lo que hace a la protección de datos personales. Se hará uso por tanto del método de caso.

Indirecta: obtención de bibliografía y cibergrafía especializada en los temas de la tesis.

Periodo que se va a estudiar

Retrospectiva: Estudio histórico de las figuras jurídicas de acceso a la información, protección de datos personales y *big data*.

Prospectiva: Análisis de la minería de datos y sus implicaciones en la forma de hacer negocios.

Análisis de los datos abiertos con el fin de detectar las formas en que las personas pueden ejercer sus derechos y también tomar decisiones.

Propósito de la Investigación

Básica o Pura: Obtener una investigación actualizada con los derechos de acceso a la información y protección de datos personales, los cuales siguen generándose tanto leyes generales, leyes específicas, así como normas secundarias tales como acuerdos, lineamientos, manuales, etc.

Aplicada: A partir de la investigación documental generar información que se pueda aplicar en la forma en que los sujetos obligados pueden cumplir con las nuevas obligaciones de transparencia.

Proponer opciones para que los particulares cumplan con las obligaciones inherentes a la protección de datos personales en posesión de particulares.

Métodos de Investigación

Métodos Teóricos de Investigación

Método Histórico – Lógico. Se aplica en el estudio de las figuras de acceso a la información, protección de datos personales y *big data*.

Se utiliza la lógica para el sentido de estudio de cada figura por medio de la cronología de acontecimientos realizando las valoraciones retrospectivas de las figuras jurídicas de estudio.

Método Análisis – Síntesis. Este método posibilita descomponer el objeto que se estudia en sus elementos para luego recomponerlo a partir de la integración de éstos, y destacar el sistema de relaciones existente entre las partes y el todo en este sentido cada una de las figuras a estudio se analizarán en sus partes, en sus procedimientos, en sus formas de aplicación y en sus formas de interacción.

Método Inductivo – Deductivo. Se empleará en el estudio de las tesis interpretativas de los tribunales en cuanto al uso de acceso a la información.

Método sistémico – estructural – funcional. Se utilizará la base de teoría de sistemas de Luhmann aplicado al modelo del Sistema Nacional de Transparencia de acuerdo con la Ley General de Transparencia y Acceso a la Información Pública.

Método de derecho comparado.

Se utiliza el método externo de estudio al acceso a la información con respecto a España, Estados Unidos y Argentina.

Se emplea un método comparado interno con respecto a legislaciones generales, federales y estatales.

Métodos empíricos de investigación

Método de análisis de contenido. Se aplicará al analizar el *big data*, sus tendencias y sus posibles implicaciones.

Hermenéutico. Se utiliza en la interconexión de los sistemas de acceso a la información y en el engarce sistémico entre los sistemas de datos personales y *big data*.

Capítulo 1. Desarrollo Histórico Conceptual del Big Data, Datos Personales y del Acceso a la Información Pública Gubernamental

1.1 Evolución del Big Data

Si bien en neologismo *Big Data,* ya está en el lenguaje común, considero que para entenderlo en su totalidad será necesario conocer algunos conceptos clave que son necesarios, tales como: Datos, información, *big data*, y minería de datos.

Comencemos con el primer concepto: **Dato**. En primer lugar, el diccionario de la Real Academia Española nos indica los siguiente: Del lat. *datum* 'lo que se da'. Cabe advertir que en el desarrollo de los conceptos, solo se utilizarán aquellos que sean más afines con el desarrollo de la presente investigación.

> 1. m. Información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho. *A este problema le faltan datos numéricos*.
>
> 3. m. *Inform*. Información dispuesta de manera adecuada para su tratamiento por una computadora.[2]

Por su parte el diccionario Oxford indica: MASCULINE NOUN

> 1. Información concreta sobre hechos, elementos, etc., que permite estudiarlos, analizarlos o conocerlos.
>
> *Los datos del censo; el análisis aportó datos de gran interés respecto a la génesis de esta fobia; cada ficha contiene los datos comerciales, fiscales y estadísticos de cada proveedor; estos datos configuran una densidad de población débil, aunque ello no descarta que haya núcleos muy poblados y muchas regiones vacías*
>
> 2. Computing
> Cifra, letra o palabra que se suministra a la computadora como entrada y la máquina almacena en un determinado formato.
>
> *Al introducir palabras o números en una hoja de cálculo, la computadora los procesa y los almacena como datos en código binario*.[3]

Para terminar este concepto, y solo como fines indicativos, en la página de conocimiento colectivo conocida como *Wikipedia*, se define como dato:

> Un dato es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.

[2] DATO. En: Real Academia Española, *Diccionario de la Real Academia Española*, 2021, [fecha de consulta: 3 de diciembre de 2022]. Disponible en: *https://dle.rae.es/dato*
[3] DATO. En Oxford, *Diccionario Léxico Oxford*, 2020, [fecha de consulta: 5 de octubre de 2021]. Disponible en: *https://www.lexico.com/es/definicion/dato*

> […] Los datos pueden consistir en números, estadísticas o proposiciones descriptivas. Los conceptos de datos, información, conocimientos y sabiduría están inter-relacionados, los datos convenientemente agrupados, estructurados e interpretados se han considerado que son la base de la información humanamente relevante que se pueden utilizar en la toma de las decisiones, la reducción de la incertidumbre o la realización de cálculos. […] Se ha dicho que datos son el nuevo petróleo de la economía digital.[4]

Llama la atención el hecho que el origen de la palabra dato corresponda con el de dar; es decir, que un dato proporciona "algo", que puede ser cualquier cosa, un número, una frase, una imagen; etc.; además, un dato no representa nada realmente hasta que se procesa, ya que este procesamiento es lo que da sentido a los datos y tipos de datos (Cualitativos o cuantitativos), es lo que proporciona la información, una información que posteriormente será utilizada para distintos fines.

El segundo concepto clave es el de **información**. Para la Real Academia Española es uno de los conceptos que más significados tiene. Proviene del latín *informatio, -ōnis* 'concepto', 'explicación de una palabra'.

> 5. f. Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada.
> 6. f. Conocimientos comunicados o adquiridos mediante una información.
> Información de *vita et moribus*
> 1. f. información que se hacía de la vida y costumbres de aquel que había de ser admitido en una comunidad o antes de obtener una dignidad o cargo.
> Información en derecho
> 1. f. Der. Alegato extraordinario impreso, con el cual, a veces, en apelación civil de mayor cuantía, se sustituyen los informes orales de las partes litigantes.
> Información parlamentaria
> 1. f. Investigación sobre algún asunto importante, encargada a una comisión especial de cualquiera de los cuerpos colegisladores.
> Información privilegiada
> 1. f. Información que, por referirse a hechos o circunstancias que otros desconocen, puede generar ventajas a quien dispone de ella.
> 2. f. Der. En el ámbito de los mercados de valores, información a la que se ha tenido acceso reservadamente, con ocasión del desempeño de un cargo o del ejercicio de una actividad empresarial o profesional, y que, por su relevancia para la cotización de los valores, es susceptible de ser utilizada en provecho propio o ajeno.[5]

Para el Diccionario Oxford significa: FEMININE NOUN

1. Acción de informar.

---

[4] DATO. En colaboradores de Wikipedia. *Wikipedia, La enciclopedia libre*, 2022, [fecha de consulta: 3 de diciembre de 2022]. Disponible en: *https://es.wikipedia.org/w/index.php?title=Dato&oldid=131429421*

[5] INFORMACIÓN. En Real Academia Española, *Diccionario de la Real Academia Española*, 2021, [fecha de consulta: 3 de diciembre de 2022]. Disponible en: *https://dle.rae.es/informaci%C3%B3n?m=form*

Cualquier país democrático tiene leyes que garantizan la libertad de información

2. Noticia o dato que informa acerca de algo.

El gobierno israelí recibió información acerca de dos de sus siete soldados desaparecidos; el periódico dispone de corresponsales distribuidos por todos los países que recogen las informaciones y las transmiten con la mayor rapidez
.

3. Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada.[6]

En la Wikipedia se puede encontrar una parte interesante en cuanto a la parte que señala que "los datos sensoriales una vez percibidos y procesados constituyen una información que cambia el estado de conocimiento, eso permite a los individuos o sistemas que poseen dicho estado nuevo de conocimiento tomar decisiones pertinentes acordes a dicho conocimiento." [7]

Por su parte para Daniel Soto Gama el concepto de información se entiende de la siguiente manera:

> […] la información es el conjunto de datos o conocimientos, a los que habiéndoseles dado forma y estructura determinada traen consigo un mensaje. Informar es la acción de dar a conocer precisamente ese conjunto de datos estructurados. Para J. Antonio Paoli, quien estudia a la información a partir del proceso de comunicación, ésta representa un conjunto de mecanismos necesarios que hacen posible al individuo retomar los datos que se encuentran en el medio en el que se desenvuelve para una vez estructurándolos de una manera determinada le sirvan de guía de acción." [8]

De lo anterior se puede percibir diferentes connotaciones de lo que es la información:

[6] Información Oxford, *Diccionario Léxico Oxford*, 2021, [fecha de consulta: 5 de octubre de 2021]. Disponible en: *https://www.lexico.com/es/definicion/dato*
[7] Colaboradores de Wikipedia. "Información" *Wikipedia, La enciclopedia libre*, 2022, [fecha de consulta: 3 de diciembre de 2022]. Disponible en: *https://es.wikipedia.org/w/index.php?title=Informaci%C3%B3n&oldid=131923412*
[8] Soto Gama, Daniel, *Principios Generales del Derecho a la Información*, [en línea] México, INFOEM, 2010, [fecha de consulta: 3 de diciembre de 2022]. Disponible en *https://www.infoem.org.mx/sipoem/ipo_capacitacionComunicacion/pdf/pet_tesis_003_2009.pdf* p. 25.

Imagen: Información.
Fuente: Elaboración propia.

El cuadro anterior, sintetiza las diferentes formas de acercarnos a la información como objeto de estudio desde diferentes ópticas, ya sea, política, informática, filosófica, gramatical y etimológica; esto abre paso a entender que históricamente la humanidad le ha dado un valor fundamental a la información a tal grado que muchos han muerto por obtener información; es decir, que el devenir histórico de la información va desde la más estricta opacidad o cómo se le llegó a conocer en la antigua Roma como *Arcana Imperi*, hasta la actualidad donde toda la información es pública tocante a sujetos obligados, y con reglas estrictas de clasificación de la información, donde solo en casos expresamente señalados en las leyes, la información se debe mantener al margen de los ciudadanos.

Y es que, si vemos la información desde un punto de vista filosófico-político, la información es tanto conocimiento, como poder; o bien, la posibilidad de poder hacer algo con esa información. Al parecer fue Hobbes, en su libro intitulado “El Leviatán”, quien puso en circulación la idea de que «quien tiene la información, tiene el poder».

> Conviene recordar que la información no es conocimiento. Si lo fuese, cualquiera que entrase en una biblioteca sería sabio al disponer de tanta información como contienen los libros y para qué hablar de la información accesible a través de internet. Pero tanta información no hace a nadie sabio, falta algo que sólo los sabios, los maestros, poseen y transmiten: organización, estructuración, separación de la información esencial de la accesoria, criba del grano y la paja.
> La frase de Hobbes remite a la información, no al conocimiento. Pero no a cualquier información, no a la que podemos adquirir a raudales con un golpe

> de click, a través de internet, por ejemplo. No, ya se entiende que se trata de la denominada “información privilegiada”.[9]

Ahora bien, si se considera que la información es también conocimiento valdría la pena entender el pensamiento de Francis Bacon, el cual, su obra *Meditationes Sacrae* escrito en el año 1597 se encuentra el aforismo latino *ipsa scientia potestas est* que es traducido literalmente como 'el conocimiento en su poder', luego reinterpretado como "el conocimiento es poder".

> "El conocimiento es poder" significa que, mientras más conocimiento una persona tenga sobre algo o alguien, más poder tendrá. Grosso modo, la frase se refiere a cómo el conocimiento sobre algo nos entrega más opciones y mejores maneras de enfrentar la situación.
> Francis Bacon ejemplifica esto señalando el absurdo de las disputas sobre los límites del conocimiento de Dios versus los límites de su poder, ya que el conocimiento en sí mismo es un poder, por lo tanto, si su poder es ilimitado, su conocimiento también lo será. Francis Bacon explica además la relación del conocimiento y la experiencia en la siguiente frase: “El conocimiento se adquiere leyendo la letra pequeña de un contrato; la experiencia, no leyéndola.”[10]

También hay quien afirma que el aforismo de Bacon es “La información es conocimiento”, dándole así un concepto más “fino y humanista”. [11]

Sea como sea, hoy vivimos en la llamada era de la información una era que se caracteriza por lo siguiente:

1) Aumento de el volumen de los datos disponibles;
2) Cambio de comunicación lineal en interactiva;
3) Amplio concepto de alfabetización;
4) Fusión del proceso de la información y de la tecnología del transporte;
5) Reglamentación de las nuevas tecnologías;
6) Libertad e intimidad;
7) Relación entre la información disponible y su uso;

---

[9] Martínez Alpañez, Rubén, “La información es poder”, *La opinión de Murcia,* Opinión, España, Espacio Abierto, 2014, [fecha de consulta: 3 de diciembre de 2022]. Disponible en *https://www.laopiniondemurcia.es/opinion/2014/03/27/informacion/546861.html*

[10] Chen, Caterina, “El conocimiento es poder”, *Cultura Genial*, Frases y Discursos, [fecha de consulta: 3 de diciembre de 2022]. Disponible en *https://www.culturagenial.com/es/el-conocimiento-es-poder/#:~:text=%22El%20conocimiento%20es%20poder%22%20significa,o%20alguien%2C%20m%C3%A1s%20poder%20tendr%C3%A1.&text=Francis%20Bacon%20(1561%2D1626)%3A,para%20promover%20la%20ciencia%20aplicada.*

[11] Javier Acuña, Francisco, “¿Información es poder? No, puede ser mucho más útil”, *El Financiero*, Secc. Opinión, México, junio, 2020, [fecha de consulta: 3 de diciembre de 2022]. Disponible en *https://www.elfinanciero.com.mx/opinion/francisco-javier-acuna/informacion-es-poder-no-puede-ser-mucho-mas-util*

8) Variedad y limitación entre medios y sociedad.[12]

Cabe destacar que, en esta etapa, la información es gestionada dentro de una sociedad que se puede catalogar ya sea como sociedad de la información o como sociedad informacional. Al respecto Manuel Castell nos señala:

> El término sociedad de la información destaca el papel de esta última en la sociedad. Pero yo sostengo que la información, en su sentido más amplio, es decir, como comunicación del conocimiento, ha sido fundamental en todas las sociedades, incluida la Europa medieval, que estaba culturalmente estructurada y en cierta medida unificada en torno al escolastismo (*sic)*, esto es, en conjunto, un marco intelectual (véase Southern, 1995). En contraste, el término informacional indica el atributo de una forma específica de organización social en la que la generación, el procesamiento y la transmisión de a información se convierten en las fuentes fundamentales de la productividad y el poder, debido a las nuevas condiciones tecnológicas que surgen en este periodo histórico. Mi terminología trata de establecer un paralelo con la distinción entre industria e industrial. Una sociedad industrial (noción habitual en la tradición sociológica) no es sólo una sociedad en la que hay industria, sino aquella en la que las formas sociales y tecnológicas de la organización industrial impregnan todas las esferas de la actividad, comenzando con las dominantes y alcanzando los objetos y hábitos de la vida cotidiana. La utilización que hago de los términos sociedad informacional y economía informacional intenta caracterizar de modo más preciso las transformaciones actuales más allá de la observación de sentido común de que la información y el conocimiento son importantes para nuestras sociedades. Sin embargo, el contenido real de «Sociedad informacional» ha de determinarse mediante la observación y el análisis. Éste es precisamente el objetivo de este libro. Por ejemplo, uno de los rasgos clave de la sociedad informacional es la lógica de interconexión de su estructura básica, que explica el uso del concepto de «sociedad red», definido y especificado en la conclusión de este volumen. No obstante, otros componentes de la «sociedad informacional», como los movimientos sociales o el Estado, presentan rasgos que van más allá de la lógica de la interconexión, aunque están muy influidos por ella al ser característica de la nueva estructura social. Así pues, «la sociedad red» no agota todo el significado de la «sociedad informacional».[13]

Como forma de corolario de este pequeño apartado de la era de la información, cabe añadir que ahora se dice que la era de la información es ya un concepto rebasado, ahora todo se maneja como reputación en la entrega de la información. Al respecto Gloria Origgi nos señala:

---

[12] D. Ruben, Brent, “En la era de la información: información, tecnología y estudio del comportamiento”, [en línea] EUA, Rutgers University, 1990, [fecha de consulta: 3 de diciembre de 2022]. Disponible en
En la era de la información: información, tecnología y estudio ...revistas.ucm.es › index.php › DCIN › article › download, p. 57.

[13] Castells, Manuel, *La era de la información. Economía, sociedad y cultura*. Vol. 1 México siglo XXI, 1996, [fecha de consulta: 3 de diciembre de 2022]. Disponible en
http://www.economia.unam.mx/lecturas/inae3/castellsm.pdf p. 14

> Experimentamos un cambio paradigmático fundamental en nuestra relación con el conocimiento. Estamos pasando de la "era de la información" a la "era de la reputación", donde la información tendrá valor solo si está ya filtrada, evaluada y comentada por otros. Hoy día, la reputación se ha convertido en el pilar fundamental de la inteligencia colectiva. Es la guardiana del conocimiento, y las llaves para abrir esa puerta las tienen otros. La manera en que la autoridad del conocimiento se construye en la actualidad nos hace dependientes de las opiniones inevitablemente subjetivas de otras personas, que generalmente no conocemos.
>
> Daré algunos ejemplos de esta paradoja. Si alguien te pregunta por qué crees que están ocurriendo cambios en el clima que pueden dañar la vida en la Tierra, la respuesta más razonable que puedes dar es decir que te fías de la reputación de las fuentes a las que normalmente acudes para informarte sobre la seguridad del planeta. En el mejor de los casos, confías en la reputación de las investigaciones científicas y crees que la revisión por pares es una manera razonable de filtrar o separar las "verdades" de las hipótesis falsas o las tonterías.
>
> Pero lo más fácil es decir que confías en los periódicos, revistas o canales de televisión que tienen un sesgo ideológico que apoya la investigación científica para que te resuman sus descubrimientos. En este último caso, estás doblemente distanciado de las fuentes: te fías de la confianza de otra gente en la ciencia.[14]

De esta manera, llegamos al tercer concepto que nos ocupa, denominado **Minería de Datos**. "La minería de datos se relaciona con las técnicas y las herramientas utilizadas para extraer información útil de grandes volúmenes de datos."[15] "La Minería de Datos (*Data Mining*) debe su nombre a la analogía entre una montaña y la gran cantidad de datos almacenados en cualquier empresa. Dentro de la montaña, ocultos entre piedras y tierra, se encuentran diamantes de gran valor que mediante actividades de minería son encontrados y aprovechados"[16]

"Al igual que un buscador de minerales remueve la tierra para encontrar pepitas de oro, la minería de datos es el proceso de clasificación de grandes conjuntos de datos para encontrar información relevante y aprovechable para una finalidad específica. Como una subdisciplina de las ciencias de la informática, la minería de datos se centra fundamentalmente en patrones."[17]

Para Witten y Frank el *Data Mining* es el "proceso de extraer conocimiento útil y

[14] Origgi, Gloria, "Terminó la era de la información, ahora todo es reputación" *Revista Letras Libres*, México, 03 de mayo de 2018, [fecha de consulta: 3 de diciembre de 2022]. Disponible en *https://www.letraslibres.com/espana-mexico/revista/termino-la-era-la-informacion-ahora-todo-es-reputacion*

[15] UNAM, *Introducción a la minería de Datos*, México, UNAM, enero 2020, [fecha de consulta: 3 de diciembre de 2022]. Disponible en *https://docencia.tic.unam.mx/presenciales/Introduccion-a-la-mineria-de-datos.html*

[16] Beltrán Martínez, Beatriz, "Minería de Datos", México, BUAP, [fecha de consulta: 3 de diciembre de 2022]. Disponible en *http://bbeltran.cs.buap.mx/NotasMD.pdf* p.18

[17] s/a, "¿Qué es la minería de datos?" Kaspersky, s/d, [fecha de consulta: 3 de diciembre de 2022]. Disponible en *https://latam.kaspersky.com/resource-center/definitions/data-mining*

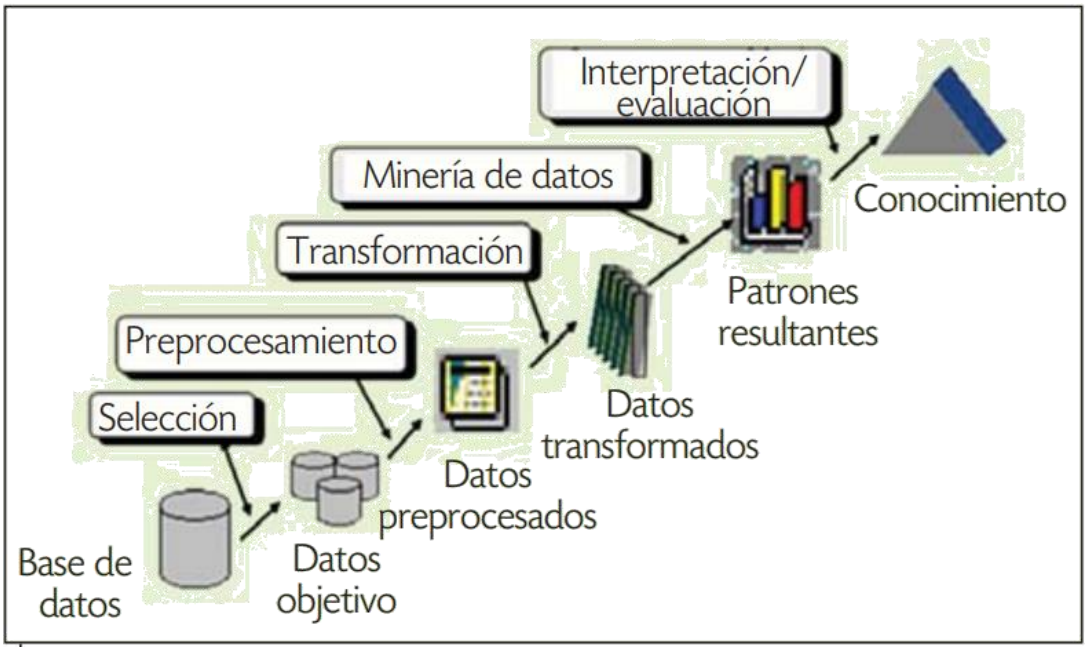
comprensible, previamente desconocido, desde grandes cantidades de datos almacenados en distintos formatos."[18]

Asimismo, para Hand, Mannila y Smyth, la minería de datos consiste en el "análisis de grandes volúmenes de Datos para encontrar relaciones no triviales, y para resumirlos de manera que sean entendibles y útiles."[19]

Por su parte, para Hand, es la "extracción de patrones y modelos interesantes, potencialmente útiles y datos en base de datos de gran tamaño"[20]

"Este sistema tienen como finalidad prevenir a los directivos de empresas sobre situaciones interesantes, anómalas e incluso peligros no detectados con anticipación. Los llamados "mineros" son auxiliares indispensables para el ejecutivo de cualquier empresa bien organizada"[21]

La minería de datos se especializa en realizar tareas con ayuda de una computadora, apoyándose en un modelo de trabajo o proceso que se ha construido



en una secuencia determinada como la que se aprecia continuación:[22]

[18] Citado por, Aguilar, José, "Introducción a la Minería de Datos, Metodologías y Técnicas de Minería de Datos", Venezuela, Universidad de los Andes, [fecha de consulta: 3 de diciembre de 2022]. Disponible en *http://www.ing.ula.ve/~aguilar/actividad-docente/IN/transparencias/clase40.pdf* p. 1

[19] *Ídem*

[20] *Ídem*

[21] Martínez Luna, Gilberto Lorenzo, "Minería de Datos: cómo hallar una aguja en un pajar", *Revista Ciencia*, [en línea] Vol. 62, No. 3. Julio-septiembre 2011, CONACYT-Academia Mexicana de Ciencias, [fecha de consulta: 3 de diciembre de 2022]. Disponible en *https://www.revistaciencia.amc.edu.mx/images/revista/62_3/PDF/mineria_aguja.pdf* p. 18.

[22] *Ídem*

Imagen: Fases del proceso de descubrimiento en bases de Datos.
Tomada de: Martínez Luna, Gilberto Lorenzo, *Minería de Datos: cómo hallar una aguja en un pajar*. Disponible en: *https://www.revistaciencia.amc.edu.mx/images/revista/62_3/PDF/mineria_aguja.pdf* p. 22.

A la par de este concepto de minería de Datos, existe también uno que se ha ido desarrollando como un sinónimo de este. El término *Knowledge Discovery in Databases* o KDD "acuñado en 1989, se refiere a todo el proceso de extracción de conocimiento a partir de una base de datos y marca un cambio de paradigma en el que lo importante es el conocimiento útil que seamos capaces de descubrir a partir de los datos"[23]

> En el primer estado del arte sobre el área [Fayy96] se dice:
>
> "La mayoría de los trabajos previos en KDD, se centraban en […] la etapa de Minería de Datos. Sin embargo, los otros pasos son de considerable importancia para el éxito de las aplicaciones de KDD en la práctica." Lo que claramente apunta a la importancia de incluir en la metodología el preproceso de los datos, o la formalización del conocimiento descubierto.
>
> En realidad, los términos MD y KDD son a menudo confundidos como sinónimos. En general se acepta que la MD es un paso particular en el proceso consistiendo en la aplicación de algoritmos específicos para extraer patrones (modelos) de los datos. Otros pasos en el proceso KDD, son la preparación de los datos, la selección y limpieza de los mismos, la incorporación de conocimiento previo, y la propia interpretación de los resultados de minería. Estos pasos aplicados de una manera iterativa e interactiva aseguran que un conocimiento útil se extraiga de los datos.[24]

Algunas de las tareas de la minería de datos incluyen la identificación de aplicaciones para técnicas existentes y desarrollo de nuevos patrones como el comercio electrónico y la bioinformática. "Existen numerosas áreas donde la minería de datos se puede aplicar, prácticamente en todas las actividades humanas que generen datos:"[25]

[23] *Cfr*. Riquelme, José C.; Ruiz, Roberto; Gilbert, Karina, "Minería de Datos: Conceptos y Tendencias", Inteligencia Artificial. [en línea] Revista Iberoamericana de Inteligencia Artificial, vol. 10, núm. 29, primavera,
España, 2006, [fecha de consulta: 3 de diciembre de 2022]. Disponible en *https://www.redalyc.org/pdf/925/92502902.pdf* pp. 11-18,
[24] *Ídem*
[25] *Ídem*

Imagen: Minería de Datos.
Elaboración propia. Tomada a partir de Riquelme, Ruiz y Gilbert, Minería de Datos: Conceptos y tendencias. [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.redalyc.org/pdf/925/92502902.pdf* pp. 11-17

Adicionalmente, la minería de datos se utiliza para muchos fines, según cada empresa y sus necesidades. Entre algunos de sus usos posibles se incluyen los siguientes:

Pronósticos y riesgos: analizar datos para determinar el origen de desaciertos pasados (por ejemplo, la cantidad de visitantes web que no compraron un determinado artículo después de examinarlo) podría ayudar a un minorista a tomar mejores decisiones sobre las adquisiciones de inventario en el futuro. Del mismo modo, determinar la hora del día en que un sistema experimentó una sobrecarga de tráfico web en el pasado podría ayudar a un negocio a estar mejor preparado mediante la asignación de más recursos o la inversión en actualizaciones de servidor.

Agrupación: los datos proporcionados por los clientes les permiten a las empresas agrupar usuarios de muchas maneras; por ejemplo, demográficamente en función del sexo, la edad, los ingresos, el lugar en el que viven y sus hábitos de consumo. Esto les permite dirigirse eficientemente a los usuarios adecuados con ofertas o mensajes específicos.

Análisis de comportamiento: examinar los datos les permite a las empresas comprender el tipo de estímulos a los que los clientes responden. ¿Responden ciertos grupos a ofertas específicas o correos electrónicos a una determinada hora del día o en un día determinado de la semana, por ejemplo? O bien, quizá proporcione claridad sobre qué motiva a los usuarios a visitar un sitio web y no

> otro, o sobre por qué desisten de comprar en el último minuto. El análisis ayuda a determinar qué se puede hacer para evitar los comportamientos negativos de los consumidores que perjudican a su empresa.[26]

Por su parte, los mineros o exploradores de datos a la hora de llevar a cabo un análisis de *Data Mining*, deberán realizar cuatro pasos distintos:

1. Determinación de los objetivos: El cliente determina qué objetivos quiere conseguir gracias al uso del *Data Mining*.
2. Procesamiento de los datos: Selección, limpieza, enriquecimiento, reducción y transformación de la base de datos.
3. Determinación del modelo: Primero se debe hacer un análisis estadístico de los datos y después visualización gráfica de los mismos.
4. Análisis de los resultados: En este paso se deberán verificar si los resultados obtenidos son coherentes.[27]

El siguiente concepto clave es el de *Big Data*, que si bien se abordará al completo en el capítulo 2 en este capítulo solo tocaremos algunas definiciones:

> La traducción literal de la expresión Big Data es: "Datos Masivos" o "datos a gran escala". Según Ziff Davis, fundador de ZDNet, Big Data es un término que aplica a toda la información que no puede ser procesada o analizada mediante procesos tradicionales; es decir, las cantidades masivas de datos que se acumulan con el tiempo que son difíciles de analizar y manejar utilizando herramientas comunes de gestión de bases de datos. Así mismo (*sic*), algunas definiciones más extensas también incluyen al tratamiento y análisis de estos enormes repositorios de datos.[28]

Otra definición del Diccionario de Economía On Line "El Economista.es" indica: "Denominamos Big Data a la gestión y análisis de enormes volúmenes de datos que no pueden ser tratados de manera convencional, ya que superan los límites y capacidades de las herramientas de software habitualmente utilizadas para la captura, gestión y procesamiento de datos."[29]

A su vez, el Diccionario panhispánico del español jurídico refiere por *big data*: *Tel*. Conjunto de técnicas que permiten analizar, procesar y gestionar conjuntos de datos extremadamente grandes que pueden ser analizados informáticamente para revelar

---

[26] s/a, "¿Qué es la minería de datos?" Kaspersky, s/d, *https://latam.kaspersky.com/resource-center/definitions/data-mining vid*. Nota 16.

[27] Ribas, Ester, "¿Qué es el Data Mining o minería de datos?", España, IEBS, 2018, [fecha de consulta: 3 de diciembre de 2022] Disponible en https://w*ww.iebschool.com/blog/data-mining-mineria-datos-big-data/*

[28] Bautista Villagómez, Diana, "Big Data: El poder de la información", México, IEXE, Universidad en línea, 2018, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.iexe.edu.mx/ciencia-y-tecnologia-blog/big-data-el-poder-de-la-informacion.html*

[29] BIG DATA. En: el Economista, *Diccionario de Economía*, El economista.es, España, s/d., [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.eleconomista.es/diccionario-de-economia/big-data*

patrones, tendencias y asociaciones, especialmente en relación con la conducta humana y las interacciones de los usuarios.[30]

Gartner definió *big data* como "activos de información caracterizados por su volumen elevado, velocidad elevada y alta variedad, que demandan soluciones innovadoras y eficientes de procesado para la mejora del conocimiento y la toma de decisiones en las organizaciones."[31]

Ahora bien, una vez que se han abordado los conceptos clave de este capítulo, se pasará a abordar la evolución del *big data*.

"Su historia se remonta al nacimiento de las primeras herramientas informáticas que llegaron en 1940. En esta misma década comenzaron a aparecer programas que eran capaces de predecir posibles escenarios futuros. Por ejemplo, el equipo del Proyecto Manhattan (1944) que realizaba simulaciones por ordenador para predecir el comportamiento de una reacción nuclear en cadena."[32]

> En las seis décadas transcurridas desde la segunda Guerra Mundial, las Ciencias Naturales y las Ciencias Humanas han ido acumulando inmensos tesoros de datos cuantificables que raramente son objeto de confrontación. […] A partir de las primeras extracciones de núcleos de hielo en la década de 1960 se han venido acumulando de modo permanente *big data* de los más variados orígenes; luego, unos modelos de base informática han convertido los datos reunidos en el ámbito de la meteorología en posibles propuestas acerca de la manera en que nuestra atmósfera ha ido cambiando en relación con la contaminación.[33]
>
> En 1962 John W. Turkey [13] escribe "El futuro del Data Análisis" y en 1977 publica el artículo "*Exploratory Data Analysis*", en el que se argumenta que la importancia radica en el uso de los datos para sugerir hipótesis que permitan testear y explorar los mismos, permitiendo extraer conclusiones veraces. Ese mismo año la International *Association for Statistical Computing* (IASC)

[30] BIG DATA. En: Real Academia Española, *Diccionario panhispánico del español jurídico*, España, RAE, 2020, [fecha de consulta: 3 de diciembre de 2022] *https://dpej.rae.es/lema/big-data*

[31] Citado por Maté Jiménez, Carlos, "*Big Data*. Un nuevo paradigma de análisis de datos", *Revista Anales de mecánica y electricidad*, Universidad Pontificia Comillas, España, noviembre-diciembre 2014, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.iit.comillas.edu/docs/IIT-14-153A.pdf*

[32] Guerrero López, Jorge y Rodríguez Pinilla, Jorge Eduardo, "Diseño y Desarrollo de una Guía para la implementación de un ambiente Big Data en la Universidad Católica de Colombia", Universidad Católica de Colombia, 2013, Colombia, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://repository.ucatolica.edu.co/bitstream/10983/1320/1/DISE%C3%91O%20Y%20DESARROLLO%20DE%20UNA%20GU%C3%8DA%20PARA%20LA%20IMPLEMENTACI%C3%93N%20DE%20UN%20AMBIENTE%20BIG%20DATA%20EN%20LA%20UNIVERSIDAD%20CAT%C3%93LICA%20DE%20COLOMBIA.pdf* p. 20.

[33] Armitage, David y Guldi, Jo, "Grandes Problemas: Los Big Data", *Revista Cultural de Santander*, Núm. 12, España, Sección Nuevas Corrientes Intelectuales, Universidad Industrial de Santander, 2017 [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://revistas.uis.edu.co/index.php/revistasantander/article/download/8909/8794/*

establece que su misión principal consistirá en unir la estadística tradicional, la tecnología informática y el conocimiento experto, para convertir los datos en información y conocimiento.[34]

No obstante, el término "*Big Data*" es por primera vez empleado en 1997 con relación al Big Data tal y como lo conocemos ahora, en un estudio de la NASA de dos investigadores, Michael Cox y David Ellsworth , para referirse a la generación de ingentes cantidades de información cuando simulaban en los supercomputadores de la época el flujo de aire alrededor de las aeronaves. En 2001 la consultora Gartner define el modelo "V3" en la publicación "*3D Data Management: Controlling Data Volume, Velocity, and Variety*". En 2004 Google crea MapReduce, un nuevo paradigma del procesamiento distribuido de grandes cantidades de datos, un año después, en 2005 Yahoo crea la solución Hadoop para su proyecto de motor de búsqueda, basada en el funcionamiento de MapReduce de Google y *Hadoop Distributed File System* (HDFS) para el almacenamiento, posteriormente fue cedido con licencia *Open Source* a la *Apache Software Foundation* para que esta comunidad continuase su desarrollo y lo distribuyese libremente con descarga gratuita, este último hecho supone el principio de la explosión del Big Data. Ocho años después de que Michael Cox y David Ellsworth nombrasen el *Big Data* como una cantidad ingente de datos. En 2004 con el surgimiento de la web 2.0 empieza el auge de los blogs y las redes sociales y es cuando el volumen de datos empieza a aumentar exponencialmente a medida que crecen los usuarios de estas y crece el rastro de datos que a su vez estos dejan, en la web, en las redes sociales, en transacciones, en geoposicionamiento… La creciente obtención de datos es tan grande que agota el potencial de las infraestructuras IT tradicionales. [35]

En septiembre de 2005 *The National Science Board publica "Long lived Digital Data Collections: Enabling Research and Education in the 21st*" En el informe se define a los Científicos de Datos como: "informáticos, ingenieros y programadores de bases de datos y de software, expertos en estadística, bibliotecarios, y otros, cruciales para el éxito de la gestión de una colección de datos digitales".

En 2009 se publica el informe de la *Interagency Working Group on Digital "Harnessing the power of Digital Data for Science and Society"*. En él se establece que se necesita identificar y promover la aparición de nuevas disciplinas y especialistas expertos en abordar los retos complejos y dinámicos de la preservación digital, el acceso sostenido a los datos, y la reutilización de datos. Podríamos decir que los primeros análisis de datos se ejecutaron con las primeras hojas de cálculo en los años 50 para la apoyar la toma de decisiones en las empresas. Estas hojas de cálculo van evolucionando de la

[34] Instituto Gallego de Promoción Económica, *Oportunidades Industria 4.0 en Galicia*, Junta de Galicia, España, 2017, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *http://www.igape.es/gl/ser-mais-competitivo/galiciaindustria4-0/estudos-e-informes/item/download/68_b27b22a11c4f195d9d8888e875e77358*, p. 29.

[35] Galimany Suriol, Aleix y Bachs Ferrer, Jordi, *La creación de valor en las empresas a través del Big Data*, España, *Universitat* de Barcelona, 2014, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *http://diposit.ub.edu/dspace/bitstream/2445/67546/1/TFG-ADE-Galimany-Aleix-juliol15*.pdf p.8

mano de las compañías de IT y SAS, pero trabajando siempre con datos estructurados. Es, hace una década cuando, en Silicon Valley, empiezan a emerger las aplicaciones para tratar información desestructurada y poder manejar los enormes volúmenes de datos existentes hoy en día.[36]

1.2 Antecedentes de la Protección de Datos Personales

El estudio de los datos personales está íntimamente anclado a la evolución misma de los derechos humanos; si bien, en nuestra constitución mexicana dicha protección se encuentra tanto en el artículo sexto como en el artículo dieciséis; lo cierto es, que su salvaguarda ha tenido que irse "posponiendo" conforme los derechos humanos fueron evolucionando en el devenir de nuestra historia.
Bertha Solís García menciona que una de las clasificaciones de los derechos humanos es la siguiente:

a) Derechos Humanos de Primera Generación o también conocidos como Derechos Civiles y Políticos. Surgen con la Revolución Francesa como rebelión contra el absolutismo del monarca. Impone al Estado respetar siempre los Derechos Fundamentales del ser humano como es el derecho a la vida, a la libertad, a la igualdad, entre otros.
b) Derechos Humanos de Segunda Generación o Derechos Económicos, Sociales y Culturales, [DESC]. Los cuales se plantearon por primera vez en el mundo en la constitución política de los Estados Unidos Mexicanos de 1917, no sin antes haber transitado por una revolución (Revolución Mexicana de 1910). Los DESC constituyen una obligación de hacer del Estado y son de satisfacción progresiva.
c) Y los Derechos Humanos de Tercera Generación, también llamadas Derechos de los Pueblos o de Solidaridad. Surgen en nuestro tiempo como respuesta a la necesidad de cooperación internacional y regional, a la justicia internacional, al uso de los avances de las ciencias y la tecnología, a la solución de los problemas alimenticios, demográficos, educativos y ecológicos, a proteger el medio ambiente y patrimonio común de la humanidad, a contribuir el progreso que garantice la vida digna y la seguridad humana.[37]

Parte importante de los antecedentes de la Protección de los Datos personales es identificarlos en el contexto de la protección de los derechos humanos. Diferentes autores concuerdan con que la protección de los datos personales está encuadrada en los llamados derechos de la tercera generación.

---

[36] s/a, *Oportunidades Industria 4.0 en Galicia*, Junta de Galicia, España, 2017, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *http://www.igape.es/gl/ser-mais-competitivo/galiciaindustria4-0/estudos-e-informes/item/download/68_b27b22a11c4f195d9d8888e875e77358*, p. 29.
[37] Solís García, Bertha, "Evolución de los Derechos Humanos", en Moreno Bonett, Margarita y Álvarez de Lara, Rosa María, *El Estado laico y los derechos humanos en México: 1810-2010*, [en línea] México, UNAM, Instituto de Investigaciones Jurídicas, Tomo I, 2012, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://archivos.juridicas.unam.mx/www/bjv/libros/7/3100/9.pdf* p.78.

En este sentido, el profesor Aristeo García González comenta:

> […] como una estrategia reivindicatoria de los derechos humanos, se presenta una tercera generación de derechos humanos, que ha venido a cumplimentar las fases anteriores. De este modo, los derechos y las libertades de la tercera generación se presentan como una respuesta al fenómeno de lo que se ha denominado "contaminación de las libertades" —*pollution des libertés*—, término con el que algunos sectores de la teoría social anglosajona hacen alusión a la erosión y degradación que aqueja a los derechos fundamentales ante determinados usos de las nuevas tecnologías.
>
> En esta fase, y dado el desarrollo tecnológico, toma mayor auge el reconocimiento del derecho a la intimidad, por lo cual surgen así nuevos perfiles del mismo, por lo cual aquél exige un reconocimiento en sede constitucional.
>
> Por lo que ahora puede hablarse de un antes y un después de este derecho. Esto último, considerado en algunas latitudes, y para hacer frente a este fenómeno como el derecho a la libertad informática, derecho a la autodeterminación informativa, o bien, simplemente derecho a la protección de datos personales.
>
> Este nuevo derecho, y a consecuencia de las trasformaciones sociales y culturales de la sociedad y las nuevas formas de comunicación de los seres humanos, encontró su fundamento a partir del derecho a la intimidad.[38]

Ahora bien, este "neo" derecho humano, considero que está enlazado con otros derechos de la personalidad. Al respecto, en interpretación de los tribunales federales tenemos:

> PROTECCIÓN DE DATOS PERSONALES. CONSTITUYE UN DERECHO VINCULADO CON LA SALVAGUARDA DE OTROS DERECHOS FUNDAMENTALES INHERENTES AL SER HUMANO. El párrafo segundo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos reconoce los denominados derechos ARCO, relativos al acceso, rectificación, cancelación y oposición de datos personales, como un medio para garantizar el derecho de los individuos a decidir qué aspectos de su vida deben o no ser conocidos o reservados por el resto de la sociedad, y la posibilidad de exigir su cumplimiento a las autoridades y particulares que conocen, usan o difunden dicha información. Así, dichas prerrogativas constituyen el derecho a la protección de los datos personales, como un medio de salvaguarda de otros derechos fundamentales previstos en la propia Constitución y en los tratados internacionales de los que México es Parte, conforme a los cuales, el Estado tiene la obligación de garantizar y proteger el derecho de todo individuo a no ser interferido o molestado por terceros o por una autoridad, en ningún aspecto de su persona –vida privada–, entre los que se encuentra el relativo a la forma en que se ve a sí mismo y cómo se proyecta a los demás –honor–, así como de aquellos que corresponden a los extremos más personales de la vida y del entorno familiar –intimidad–, o que permiten el desarrollo integral de su personalidad como ser humano –dignidad humana–.[39]

---

[38] García González, Aristeo, "La Protección de Datos Personales: Derecho Fundamental del Siglo XXI. Un Estudio Comparado" en *Boletín Mexicano de Derecho Comparado*, [en línea] Número 120, México, UNAM, Instituto de Investigaciones Jurídicas, 2007, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://revistas.juridicas.unam.mx/index.php/derecho-comparado/article/view/3933/4971* pp. 747-748.

[39] Tesis: I.10o.A.5 CS (10a.), Semanario Judicial de la Federación, Décima Época, Tomo III,

Estos derechos que se indican es la tesis también han sido interpretados de la siguiente forma:

> DERECHOS AL HONOR, A LA INTIMIDAD Y A LA PROPIA IMAGEN. CONSTITUYEN DERECHOS HUMANOS QUE SE PROTEGEN A TRAVÉS DEL ACTUAL MARCO CONSTITUCIONAL. Si conforme a las características que conforman a los derechos humanos, éstos no recaen sobre cosas materiales, sino que otorgan acción para lograr que el Estado respete los derechos garantizados, y se consideran esenciales e inherentes al ser humano y derivados de su propia naturaleza, resulta lógico que los atributos de la personalidad se enlacen directamente con tales derechos, pues los mencionados atributos tienen una coincidencia con las libertades protegidas por los derechos del hombre como son los concernientes al honor, a la intimidad y a la propia imagen que constituyen derechos subjetivos del ser humano, en tanto que son inseparables de su titular, quien nace con ellos, y el Estado debe reconocerlos. Como no recaen sobre bienes materiales, sino sobre la personalidad de los individuos, son generales porque corresponden a todos los seres humanos, y no pueden considerarse renunciables, transmisibles o prescriptibles, porque son inherentes a la persona misma, es decir, son intrínsecos al sujeto quien no puede vivir sin ellos. Ahora, del contenido expreso del artículo 1o. constitucional se advierte que nuestro país actualmente adopta una protección amplia de los derechos humanos, mediante el reconocimiento claro del principio *pro personae*, como rector de la interpretación y aplicación de las normas jurídicas, en aquellas que favorezcan y brinden mayor protección a las personas, aunado a que también precisa de manera clara la obligación de observar los tratados internacionales firmados por el Estado Mexicano al momento de aplicar e interpretar las normas jurídicas en las que se vea involucrado este tipo de derechos, como son los señalados atributos de la personalidad conforme a la Convención Americana sobre Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos, y en casos en los que se involucra la posible afectación por daño moral de un atributo de la personalidad -en su vertiente del derecho al honor- debe aplicarse la tutela y protección consagrada en los principios reconocidos al efecto en nuestra Carta Magna, con independencia de que no exista una referencia expresa en el texto constitucional hacia la salvaguarda concreta del citado atributo, pues la obligación de protección deriva de disposiciones contenidas en dos tipos de ordenamientos superiores -Constitución y tratados internacionales- con los que cuenta el Estado Mexicano.[40]

1.2.1 En el mundo

Se reconoce en Europa los antecedentes de la Protección de Datos Personales, y su desarrollo deviene de la Declaración Universal de los Derechos del Hombre del 10 de diciembre de 1948 en París, cuyo contenido del artículo 12 versa: “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.”[41]
Mayorga-Jacome indica que

Septiembre de 2019, p. 2199.

[40] Tesis: I.5o.C.4 K (10a.), Semanario Judicial de la Federación y su Gaceta, Décima Época, Tomo 2, junio de 2013, p. 1258.

[41] Organización de las Naciones Unidas, *Declaración Universal de los Derechos Humanos*, ONU, s/d, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.un.org/es/universal-declaration-human-rights/*

> En una primera fase normativa, la protección de datos de carácter personal estaba vinculada al uso de la informática y la "afección de una serie de datos o conocimientos precisos que resultaban referibles a la esfera de intimidad del sujeto", pero muy pronto se produjo la distinción entre privacidad e intimidad, de manera que todo tratamiento de datos y recolección de los mismos en un archivo quedaba amparado por la normativa en materia de protección de datos de carácter personal.[42]

Cabe señalar que poco después de la Declaración Universal de 1948, se reconoció este derecho a la vida privada en otras declaraciones como "el Convenio para la Protección de los Derechos Humanos y Libertades Fundamentales, firmado en Roma el 14 de noviembre de 1950 (artículo 8) o el Pacto de los Derechos Civiles y Políticos, hecho en Nueva York, el 19 de diciembre de 1966 (artículos 17 y 19)"[43]

> En Europa, el Derecho a la protección de datos se perfila desde los años sesenta hasta quedar definido como el sistema de protección de datos de carácter preventivo que hoy conocemos. Se suele considerar como primer antecedente el trabajo desarrollado por el Consejo de Europa en la Resolución 509/1968 de la Asamblea del Consejo de Europa relativa a "Los derechos humanos y los nuevos logros científicos y técnicos". La citada Resolución, si bien no menciona la protección de datos directamente, concreta la necesidad de adoptar mecanismos de protección que comprenda la vida privada y otros derechos fundamentales que pueden verse afectados por las TIC. A partir de ella, se inician muchos estudios que muestran preocupación por la relación existente entre la informática y la intimidad de las personas y las implicaciones que aquellas tienen para los ciudadanos, en especial en el tratamiento de datos de carácter personal.
>
> A partir de la aprobación de aquella Resolución el Consejo de Europa no dejó de trabajar sobre este tema, y como fruto de esta labor, se aprobó un importante grupo de documentos por aquel órgano, entre los que cabe mencionar, la Resolución R (73) 22 relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado; la Resolución R (73) 23 sobre medidas de armonización en el ámbito de la informática jurídica en los Estados miembros del Consejo de Europa y la Recomendación R (74) 29. Relativa a la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector público, que establece pautas ordenadoras del sector público de la informática. Estos documentos, son considerados por la doctrina, como el verdadero origen del movimiento legislativo que se inicia en Europa y recogen los principios que aún hoy continúan vigentes, tales como la calidad de los datos (exactos y puestos al día y adecuados a la finalidad para la que se recogen), la obtención

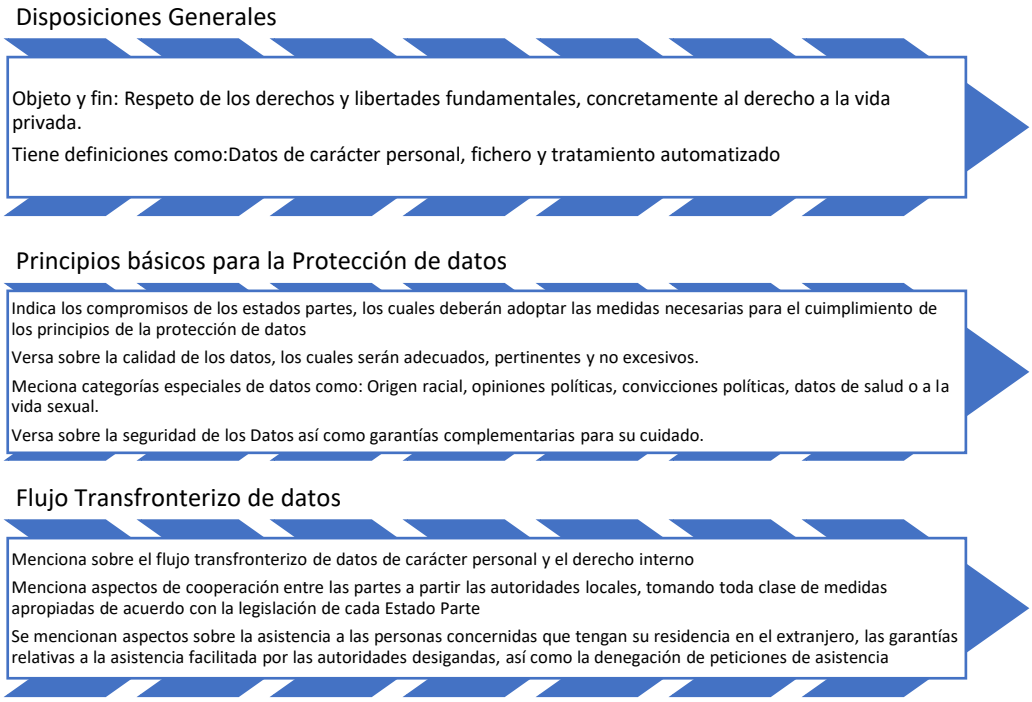
[42] Mayorga-Jácome, Tannia C. *et. al*. "Historia de la normativa reguladora de la Protección de Datos de Carácter personal en distintos países Latinoamericanos" en *Revista Dominio de las Ciencias*, México, Vol. 5, núm. 1., enero 2019, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://dominiodelasciencias.com/ojs/index.php/es/article/view/875/pdf* p. 521.
[43] Pulido Zaballos, Emilia, *La Protección de Datos Personales en España: Evolución Normativa y Criterios de Aplicación*, [en línea], España, Universidad Complutense de Madrid, 2013, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://eprints.ucm.es/22849/1/T34733.pdf* p. 87

de datos por medios legales o la adopción de medidas de seguridad en los ficheros, entre muchas otras.[44]

En el año 1990 se elabora un proyecto de Directiva europea que finalmente ve la luz en 1995 (relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos) El retraso en la adopción de esta regulación se debió a la aprobación en el ámbito internacional de dos documentos relevantes:

a) Las Directrices de la Organización para la Cooperación y el Desarrollo Económicos del año 1980, sobre protección de la privacidad y flujos transfronterizos de datos personales (Directrices OCDE)
b) El 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.[45]

De manera esquemática las partes fundamentales de este Convenio 108 son las siguientes:[46]



[44] De la Serna Bilbao, Nieves, "Lección 2: El Derecho a la Protección de Datos de Carácter Personal en Europa" *Derecho de las Tecnologías de la Información*, [en línea], España, Universidad Carlos III de Madrid, [fecha de consulta: 4 de octubre de 2021] Disponible en: *http://ocw.uc3m.es/derecho-administrativo/derecho-de-las-tecnologias-de-la-informacion/material-de-clase-1/leccion_2.pdf* pp. 4-5.
[45] *Ibidem*, p. 6.
[46] s/a, "Convenio número 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", en *Protección de Datos Personales, Compendio de lecturas y legislación*, Tiro Corto Editores, México, 2010, *https://archivos.juridicas.unam.mx/www/bjv/libros/12/5669/31.pdf* pp. 249-261.

Imagen: Convenio 108 de Europa.
Elaboración propia. Tomada a partir de Convenio número 108 del Consejo de Europa, de 28 de enero de 1981. [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://archivos.juridicas.unam.mx/www/bjv/libros/12/5669/31.pdf* pp. 249-261.

Este convenio de 28 de enero de 1981 fue tan importante, que constituyó realmente el primer instrumento internacional en materia de protección de datos, ya que "con la finalidad de garantizar a cualquier persona el respeto de sus derechos y libertades fundaménteles, independientemente de su nacionalidad o residencia, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de sus datos ("protección de datos")."[47]

> En 2006 el Consejo de Europa y la Comisión Europea tuvieron la iniciativa de establecer un Día internacional de la Protección de Datos Personales con el objetivo de ayudar a ciudadanos y empresas a comprender sus derechos y responsabilidades en materia de protección de datos, desde entonces todos los 28 de enero se conmemora la cultura de la protección de datos y se desarrollan actividades dirigidas a concienciar a los ciudadanos sobre la importancia de proteger su privacidad.[48]

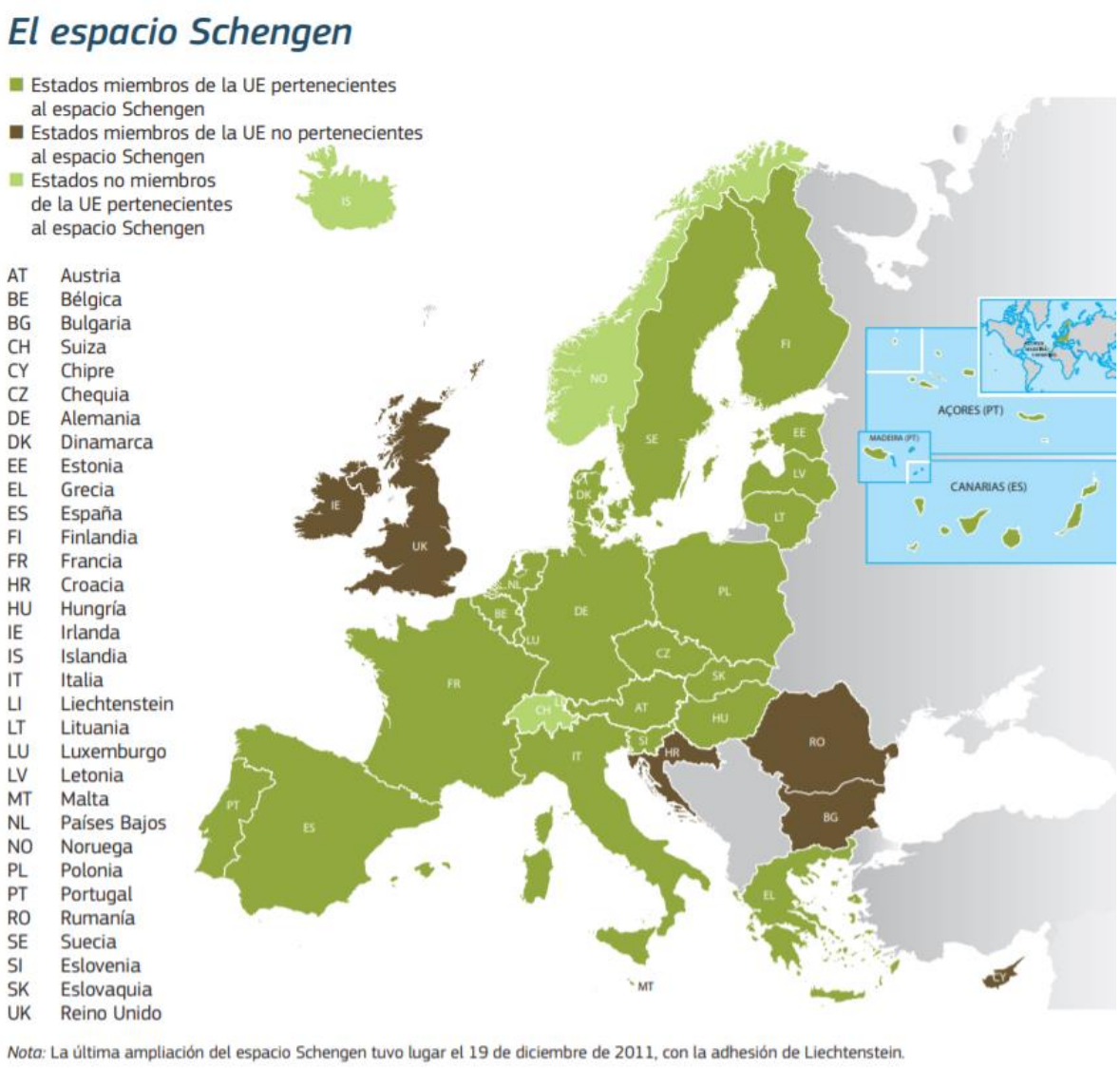
Asimismo, es importante destacar que el 12 de junio de 2018, el entonces presidente Peña Nieto, publicó el Decreto por el que se aprueba el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y su Protocolo Adicional relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos, hechos en a Estrasburgo, Francia, el 28 de enero de 1981, y el 8 de noviembre de 2001, respectivamente, de la siguiente manera:

> ARTÍCULO ÚNICO.- Se aprueba el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y su Protocolo Adicional relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos, hechos en Estrasburgo, Francia, el 28 de enero de 1981, y el 8 de noviembre de 2001, respectivamente.
> Ciudad de México, a 26 de abril de 2018.[49]

Otro momento importante en la historia de la Protección de Datos Personales es la firma del Acuerdo de Schengen, el cual lleva dicho nombre por el poblado de Luxemburgo donde la frontera de ese país confluye con las de Alemania y Francia. Aunque en principio surgió como una iniciativa entre gobiernos, la cooperación

[47] Yebra Serrano, Irene, *Día internacional de la protección de datos; 28 de enero*, España, INEAF Business School¸ 28 de enero de 2019, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.ineaf.es/tribuna/dia-internacional-de-la-proteccion-de-datos-28-de-enero/*
[48] *Ídem*
[49] s/a, *Decreto por el que se aprueba el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y su Protocolo Adicional relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos, hechos en a Estrasburgo, Francia, el 28 de enero de 1981, y el 8 de noviembre de 2001, respectivamente,* Diario Oficial de la Federación, México, 12 de junio de 2018, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.dof.gob.mx/nota_detalle.php?codigo=5526265&fecha=12/06/2018*

Schengen está ahora recogida en la normativa y legislación de la UE.
Es espacio Schengen está delimitado de la siguiente manera:[50]



Nota: La última ampliación del espacio Schengen tuvo lugar el 19 de diciembre de 2011, con la adhesión de Liechtenstein.

Imagen: Espacio Shengen.
Tomada de: Comisión Europea, *El espacio Schengen*, [fecha de consulta: 3 de diciembre de 2022] Disponible en:
https://op.europa.eu/en/publication-detail/-/publication/09fcf41f-ffc4-472a-a573-b46f0b34119e/language-es p. 2

La construcción del espacio Schengen comenzó en 1985, cuando cinco países firmaron el Acuerdo de Schengen, el cual estipulaba la supresión gradual de los controles en las fronteras comunes. Este Acuerdo fue completado por el Convenio de aplicación de Schengen de 1990, que establece la supresión definitiva de los controles en las fronteras interiores, así como una serie de medidas de acompañamiento necesarias. El Convenio reforzaba los controles en las fronteras

[50] Comisión Europea, *El espacio Schengen, La Europa sin fronteras*, Comisión Europea, 2015, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://op.europa.eu/en/publication-detail/-/publication/09fcf41f-ffc4-472a-a573-b46f0b34119e/language-es* p. 2.

exteriores, definía los procedimientos de expedición de visados uniformes, establecía el Sistema de Información de Schengen (SIS), intensificaba la cooperación policial en las fronteras interiores y mejoraba la lucha contra el tráfico de drogas.

> Sobre el particular, el Sistema de Información de Schengen (SIS) se creó para ayudar a mantener la seguridad interior en los Estados Schengen en ausencia de controles fronterizos internos. Se trata de un sistema de información a gran escala gracias al cual las autoridades policiales, de migración, judiciales y otras pueden introducir y consultar alertas con descripciones sobre personas desaparecidas, personas u objetos relacionados con infracciones penales y nacionales de terceros países a los que no les está permitido entrar o permanecer en el espacio Schengen. Por lo tanto, el SIS es una de las piedras angulares de la cooperación en la aplicación de la legislación. Al mismo tiempo, contribuye en gran medida a la protección de la frontera exterior de Schengen.
>
> Toda persona tiene derecho a acceder a sus datos personales en el SIS y solicitar que se corrijan o eliminen.[51]
>
> Otro sistema de información es el Sistema de Información de Visados, el cual es un sistema informático que conecta los consulados Schengen de terceros países con las autoridades nacionales competentes y con todos los pasos fronterizos de los Estados Schengen. Permite a las autoridades competentes de los Estados Schengen compartir información sobre solicitudes de visados; a los guardias fronterizos, verificar, mediante el uso de datos biométricos (por ejemplo, las huellas digitales), que la persona que presenta el visado es su titular legítimo, y a las autoridades competentes, identificar a las personas que se encuentran en el territorio Schengen sin documentación o con documentación falsa. También utilizan el VIS las autoridades competentes en materia de asilo.[52]

Para 1995, se emite la directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Esta Directiva considera que para eliminar los obstáculos a la circulación de datos personales, el nivel de protección de los derechos y libertades de las personas, por lo que se refiere al tratamiento de dichos datos, debe ser equivalente en todos los Estados miembros; que ese objetivo, esencial para el mercado interior, no puede lograrse mediante la mera actuación de los Estados miembros, teniendo en cuenta, en particular, las grandes diferencias existentes en la actualidad entre las legislaciones nacionales aplicables en la materia y la necesidad de coordinar las legislaciones de los Estados miembros para que el flujo transfronterizo de datos personales sea regulado de forma coherente y de conformidad con el objetivo del mercado interior definido en el artículo 7 A del Tratado; que, por tanto, es necesario

[51] *Ibidem*. p. 7.
[52] *Ibidem*. p. 10.

que la Comunidad intervenga para aproximar las legislaciones.[53]

En esta directiva un artículo importante era el artículo 29 del cual se desprendía el llamado Grupo de Trabajo del artículo 29 (GT Art. 29) el cual era "el grupo de trabajo europeo independiente que se ha ocupado de cuestiones relacionadas con la protección de la privacidad y los datos personales hasta el 25 de mayo de 2018 (entrada en aplicación del RGPD)."[54]

Las funciones del GT29 reconocidas por la Directiva incluían estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la Directiva, emitía dictámenes sobre el nivel de protección existente dentro de la Comunidad y en países terceros, asesoraba a la Comisión Europea sobre cualquier proyecto de modificación de la Directiva, y formulaba recomendaciones sobre cualquier asunto relacionado con la protección de datos en la Unión Europea.[55]

> El Grupo de Trabajo del artículo 29 argumentaba que el DPD[56] es la piedra angular de la rendición de cuentas y que el nombramiento de un DPD puede facilitar el cumplimiento y, además, convertirse en una ventaja competitiva para las empresas. Además de facilitar el cumplimiento mediante la aplicación de instrumentos de rendición de cuentas (tales como facilitar o llevar a cabo evaluaciones de impacto y auditorías de protección de datos), los DPD actúan como intermediarios entre las partes interesadas correspondientes (p. ej. autoridades de control, interesados y unidades de negocio dentro de una organización).[57]

En marzo de 1996 se convocó una CIG en Turín (Italia) con el objetivo de revisar el Tratado de la Unión Europea. El Tratado de Ámsterdam resultante, por el que se modifica el Tratado de la UE, los Tratados constitutivos de las Comunidades Europeas y determinados actos conexos, tuvo repercusión en materia de Datos Personales al añadirse un artículo 213 B que indica que a "partir del 1 de enero de 1999, los actos comunitarios relativos a la protección de las personas respecto del tratamiento de datos personales y a la libre circulación de dichos datos serán de

---

[53] Parlamento europeo, *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 n° L 281 de 23/11/1995 p. 0031 – 0050, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046&from=EN*

[54] Comité Europeo de Protección de Datos, *Grupo de Trabajo del artículo 29*, EDPB (*European Data Protection Board*), s/d, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://edpb.europa.eu/our-work-tools/article-29-working-party_es*

[55] *Cfr*, Agencia Española de Protección de Datos, *Qué es y quienes forman el Grupo de trabajo del artículo 29*, España, AEPD, citada por Asociación Profesional de Consultores en Protección de Datos, [fecha de consulta: 15 de septiembre de 2021] Disponible en: *https://www.apcpd.es/que-es-y-quienes-forman-el-grupo-de-trabajo-del-articulo-29/*

[56] Delegado de Protección de Datos.

[57] Agencia Española de Protección de Datos, *Directrices sobre los delegados de datos (DPD)*, [en línea], España, AEPD, Grupo de Trabajo sobre Protección de Datos del Artículo 29, 2017, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.aepd.es/sites/default/files/2019-09/wp243rev01-es.pdf* p. 4

aplicación a las instituciones y organismos establecidos por el presente Tratado o sobre la base del mismo."[58]

Derivado de esta directiva, el 18 de diciembre de 2000, se emite el Reglamento (CE) No 45/2001 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, el cual en sus diferentes considerandos dispone:

> (7) Las personas susceptibles de ser protegidas son aquéllas cuyos datos personales son tratados por las instituciones u organismos comunitarios en cualquier contexto, por ejemplo, porque estas personas estén empleadas por dichas instituciones u organismos.
>
> (8) Los principios de la protección de datos deben aplicarse a toda información relativa a una persona identificada o identificable; para determinar si una persona es identificable deben tenerse en cuenta todos los medios que razonablemente pudiera utilizar el responsable del tratamiento o cualquier otra persona para identificar a dicha persona. Los principios de la protección no deben aplicarse a los datos convertidos en anónimos de forma que la persona a quien se refieren ya no resulte identificable.
>
> (12) Debe garantizarse en toda la Comunidad una aplicación coherente y homogénea de las normas de protección de los derechos y las libertades fundamentales de las personas en lo que respecta al tratamiento de los datos personales.
>
> (13) Se trata de garantizar tanto el respeto efectivo de las normas de protección de los derechos y las libertades fundamentales de las personas como la libre circulación de los datos personales entre los Estados miembros y las instituciones y organismos comunitarios, o entre las instituciones y los organismos comunitarios, en el ejercicio de sus competencias respectivas.
>
> (14) Con este fin, es preciso adoptar disposiciones vinculantes para las instituciones y los organismos comunitarios. Tales disposiciones deben aplicarse a todo tratamiento de datos personales efectuado por las instituciones y los organismos comunitarios en la medida en que dicho tratamiento se lleva a cabo para el ejercicio de actividades que pertenecen total o parcialmente al ámbito de aplicación del Derecho comunitario.[59]

---

[58] *Tratado de Ámsterdam por el que se modifican el Tratado de la Unión Europea, los Tratados Constitutivos de las comunidades europeas y determinados actos conexos*, [en línea] Diario Oficial de las Comunidades Europeas, 10 de noviembre de 1997, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:11997D/TXT&from=ES* p. 48.

[59] *Reglamento (CE) No 45/2001 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos*, [en línea] Diario Oficial de las Comunidades Europeas, 12 de enero de 2001, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32001R0045&from=ES* pp. 1-2.

El último punto importante a tratar en este esbozo histórico, cuya principal base ha sido la legislación europea, por su importancia y trascendencia en otras legislaciones, corresponde al Reglamento General de Protección de Datos.

> El nuevo Reglamento General de Protección de Datos (RGPD) entró en vigor en mayo de 2016 y será aplicable a partir de mayo de 2018. En este periodo transitorio y aun cuando siguen vigentes las disposiciones de la Directiva 95/46 y las correspondientes normas nacionales de desarrollo, los responsables y encargados de tratamiento deben ir preparando y adoptando las medidas necesarias para estar en condiciones de cumplir con las previsiones del RGPD en el momento en que sea de aplicación.
>
> El RGPD es una norma directamente aplicable, que no requiere de normas internas de trasposición ni tampoco, en la mayoría de los casos, de normas de desarrollo o aplicación. Por ello, los responsables deben ante todo asumir que la norma de referencia es el RGPD y no las normas nacionales, como venía sucediendo hasta ahora con la Directiva 95/46.
>
> El RGPD contiene muchos conceptos, principios y mecanismos similares a los establecidos por la Directiva 95/46 y por las normas nacionales que la aplican.[60]

En sus diferentes considerandos el RGPD, reconoce lo siguiente:

> (1) La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea («la Carta») y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
>
> (2) Los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal deben, cualquiera que sea su nacionalidad o residencia, respetar sus libertades y derechos fundamentales, en particular el derecho a la protección de los datos de carácter personal. El presente Reglamento pretende contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas.
>
> (6) La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de

[60] Agencia Española de Protección de Datos, *Guía del Reglamento General de Protección de Datos para Responsables de tratamiento*, [en línea], España, AEGP, 22 de mayo de 2018, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.aepd.es/sites/default/files/2019-12/guia-rgpd-para-responsables-de-tratamiento.pdf* p. 2.

realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales.

(18) El presente Reglamento no se aplica al tratamiento de datos de carácter personal por una persona física en el curso de una actividad exclusivamente personal o doméstica y, por tanto, sin conexión alguna con una actividad profesional o comercial. Entre las actividades personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades. No obstante, el presente Reglamento se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas.

(32) El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta.

(28) La aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos. Así pues, la introducción explícita de la «seudonimización» en el presente Reglamento no pretende excluir ninguna otra medida relativa a la protección de los datos.

(110) Todo grupo empresarial o unión de empresas dedicadas a una actividad económica conjunta debe tener la posibilidad de invocar normas corporativas vinculantes autorizadas para sus transferencias internacionales de la Unión a organizaciones dentro del mismo grupo empresarial o unión de empresas dedicadas a una actividad económica conjunta, siempre que tales normas corporativas incorporen todos los principios esenciales y derechos aplicables con el fin de ofrecer garantías adecuadas para las transferencias o categorías

de transferencias de datos de carácter personal.[61]

De manera infográfica, vale la pena revisar en qué consiste el RGPD:[62]

Imagen: Reglamento sobre protección de datos.
Tomada de: Consejo Europeo, Consejo de la Unión Europea, *Infografía -Reglamento sobre protección de datos*, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.consilium.europa.eu/es/infographics/data-protection-regulation-infographics/#*

A manera de paréntesis, cabe señalar que el hecho que el Reglamento Europeo exija garantías más estrictas para las transferencias de datos personales fuera de la Unión Europea constituye una garantía ahora que WhatsApp anunció su cambio en la política de Datos Personales, los cuales indican que la transferencia de los Datos Personales no aplica para la Unión Europea.

[61] s/a, *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*, Diario oficial de la Unión Europea de 04 de mayo de 2016, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_es*

[62] s/a, *Infografía - Reglamento sobre protección de datos*, Consejo Europeo Consejo de la Unión Europea, 2015, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.consilium.europa.eu/es/infographics/data-protection-regulation-infographics/#*

Ahora bien, no solamente se debe considerar a Europa como los únicos antecedentes; sobre el particular, vale la pena observar otros países que han jugado un papel importante en el desarrollo de la protección de datos personales; de esta forma encontramos en el *common law*, a Estados Unidos, donde gracias a su esquema legal consuetudinario, se puede encontrar una de las primeras expresiones en defensa de la privacidad de Datos Personales.

Para lo anterior, vale estudiar al juez Thomas MacIntyre Cooley (1824-1898), quien en su obra "*The Elements of Torts*" (1873), definió lo que ahora denominamos derecho a la privacidad como "*the right to be let alone*", es decir, el "derecho a ser dejado solo" o de no ser perturbado o molestado por injerencias externas no deseadas. Cabe señalar que:

> Este criterio así esgrimido fue defendido en diversas oportunidades en procesos judiciales, como en el fallo de Brents vs. Morgan, señalándose en él que se trata del derecho a gozar de la soledad: "(…) el derecho que tiene cada persona de no ser objeto de una publicidad ilegal; el derecho de vivir sin interferencias ilegales del público en lo concerniente a asuntos en los cuales ese público no tiene un interés legítimo".[63]

Se dice que incluso para John Stuart Mill, había estimado un poco antes, en 1859 que: "(…) sobre sí mismo, sobre su propio cuerpo y mente, el individuo es soberano" -*over himself, over his own body and mind the individual is sovereign*-, haciendo alusión a esa capacidad autodeterminación e individualidad propia de todo ser humano.

Para 1890, E.L. Godkin mencionaba que:

> "(…) la privacidad es un producto moderno, uno de los lujos de la civilización, el cual no solo pasaba desapercibido, sino que era desconocido en las sociedades primitivas (…)"; "(…) el principal enemigo de la privacidad en la vida moderna es el interés de la gente de conocer los asuntos personales que en días después los periódicos divulgarán como chisme (…)"
>
> Agrega Godkin además "(…) mientras que la comunicación fue solamente oral se divulgaban los hechos únicamente de persona a persona, sobre un área pequeña y eran divulgados solamente en el círculo inmediato de conocidos (…)"; "(…) mientras que ahora la comunicación acerca de la privacidad es impresa, y fabrica una víctima con todos los defectos, mismos que son conocidos cientos de miles de millas de su lugar de origen, llevando la información con todos los detalles de una persona". [64]

---

[63] Clímaco Valiente, Ernesto, *Génesis histórico-normativa del derecho a la protección de los datos personales desde el derecho comparado a propósito de su fundamento*, [en línea] España, Universidad Carlo III de Madrid, 2012, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://e-archivo.uc3m.es/bitstream/handle/10016/18785/TFM_MEADH_Ernesto_Climaco.pdf?sequence=1&isAllowed=y* p. 13.

[64] *Ibidem*, p. 14

Para 1890, el “derecho a no ser dejado solo” recobra una nueva fuerza gracias al trabajo de un par de abogados de Boston, Samuel D. Warren y Louis D. Brandeis, quienes publicaron en la *Hardvard Law Review* el artículo innominado *The Right of Privacy*:

> En este artículo se recapitulaba los derechos individuales, y «… después vino el reconocimiento de la naturaleza espiritual del hombre, de sus sentimientos e intelecto. Gradualmente se ensanchó el ámbito de estos derechos y ahora el derecho a la vida significa el derecho a gozar de la vida, el derecho a estar solo; el derecho a la libertad incluye el ejercicio de otros derechos civiles, y el término «propiedad» ha llegado a incluir toda forma de posesión, intangible y tangible… Mucho después vino una protección cualificada del individuo contra ruidos y olores molestos, contra el humo, el polvo y la vibración excesiva. Se desarrollo la ley de la molestia… de la propiedad corporal derivaron los derechos incorporales abriendo el gran espacio de la propiedad intangible… Así se entendió que sólo una parte del dolor, el placer y el provecho de la vida está en las cosas físicas. Pensamientos, emociones y sensaciones demandan reconocimiento legal…»[65]

En el nacimiento del concepto de derecho a la privacidad conllevaba una parte psicológica; en este sentido tanto para Warren como para Brandeis el denominado derecho a la privacidad es el derecho de toda persona a proteger su integridad psicológica ejerciendo control sobre aquella información que afecta a la personalidad individual por reflejar su propia autoestima: “[…] el principio que ampara los escritos personales, y toda obra personal, no ya contra el robo o la apropiación física, sino contra cualquier forma de publicación, no es en realidad el principio de la propiedad privada, sino el de la inviolabilidad de la persona”.[66]

Ahora bien, para la Dra. María Nieves Saldaña, parece colocar el “dedo en la llaga” al distinguir los sentidos lingüísticos, las connotaciones y las implicaciones de las palabras intimidad en castellano; y la palabra *privacy* en la expresión anglosajona como tal, en los siguientes términos:

> En primer lugar, desde un punto de vista estrictamente lingüístico, el título del artículo tiene perfecta traducción literal a nuestra lengua, dado que el término ha sido recepcionado oficialmente en el *Diccionario de la Real Academia de la Lengua Española* con la voz de *privacidad*, definido como el «Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión», que no parece coincidir con el de intimidad, definido por una esfera más reducida en su segunda acepción, «Zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia». […]
>
> En segundo lugar, esta falta de coincidencia viene a justificar, igualmente, la

[65] Dermizaky Peredo, Pablo, “El Derecho a la intimidad”, *Ius et Praxis*,[en línea] Chile, Universidad de Talca, Vol. 6. No. 1, 2000, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.redalyc.org/pdf/197/19760113.pdf* pp. 178-179.
[66] Clímaco Valiente, Ernesto, *op cit*. Nota 62. p. 18.

elección del término *privacidad* cuando se analiza el artículo de Warren y Brandeis y su proyección en el sistema constitucional norteamericano. En efecto, aunque desde sus orígenes la formulación del derecho a la privacidad adquiere una connotación caracterizada por el rechazo de toda intromisión no consentida en la vida privada, especialmente del Estado y los medios de comunicación, haciendo prevalecer las ideas de aislamiento y autonomía, sin embargo, la aproximación al concepto de privacidad en la cultura jurídica norteamericana ha dependido de factores sociológicos, culturales y temporales que han dificultado una definición unánimemente aceptada, repercutiendo en los diferentes ámbitos constitucionales protegidos. Así, se ha formulado la *privacidad* en términos de anonimato y soledad, de secreto, atendiendo a los conceptos de autonomía, individualidad, desarrollo de la personalidad, y como sustrato esencial de la inviolable dignidad personal, y, recientemente, se reivindica como derecho de control sobre el flujo de la información personal.

La dificultad para definir con precisión el ámbito de la privacidad ha motivado que la jurisprudencia norteamericana de 1787 ni sus enmiendas mencionan expresamente el derecho a la privacidad (*right to privacy*), sin embargo, el Tribunal Supremo, a lo largo de una amplia y fluctuante jurisprudencia, lo ha considerado implícito en la libertad de asociación que ampara la Primera Enmienda, que salvaguarda frente a cualquier obligación legal de revelar la pertinencia a un grupo u organización; en la garantía de la Cuarta Enmienda frente a registros y requisas arbitrarias (*unreasonable searches and seizures*), que limita la intrusión del gobierno en las personas, domicilios, documentos y efectos personales, incluyéndose no sólo los supuestos de invasión material (*physical trespass*) sino también de vigilancia electrónica; en la Quinta Enmienda, que protege frente a la incriminación contra uno mismo y la obligación de revelar información personal; en la reserva de derechos del pueblo que reconoce la Novena Enmienda; y en el concepto de libertad sustantiva que el Tribunal Supremo ha interpretado ampara la cláusula del debido proceso legal (*due process of law*) de la Decimocuarta Enmienda, que garantiza el derecho fundamental de la persona a la autonomía en la toma de decisiones de especial relevancia para el desenvolvimiento de la personalidad individual sin injerencia estatal alguna, lo que le ha otorgado una «posición preferente» que impone a toda la legislación que pretenda su restricción demostrar una extraordinaria justificación, esto, es, un interés estatal relevante (*compelling state interest*), incluyéndose el derecho a contraer matrimonio, a tener hijos y decidir sobre la educación y crianza de éstos, al uso de anticonceptivos, el derecho al aborto y a la libertad sexual en el ámbito privado, planteándose incluso si la cláusula del debido proceso ampara el derecho a rechazar un tratamiento médico y a una muerte digna, y, finalmente en la década de los sesenta emerge una jurisprudencia vacilante que tiende a incluir en la zona de privacidad protegida constitucionalmente por el concepto de libertad de la Decimocuarta Enmienda el interés individual en evitar la divulgación de información personal, la llamada «*informational privacy*»

Por tanto, la noción de privacidad con la que se designa la protección de la esfera privada de la persona en los Estados Unidos presenta unos contornos más amplios que la concepción de la intimidad imperante en el ámbito

> europeo y español, de carácter más restringido, de ahí que sea preferible recurrir al término de privacidad, que se aproxima en su acepción al significado y contenido más extenso del homólogo inglés, al identificarse con el ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión.
>
> Y en tercer lugar, la opción por el término *privacidad* se justifica porque lo que se pretende en estas páginas es analizar el artículo de Warren y Brandeis desde la perspectiva del Derecho constitucional de los Estados Unidos, entendiendo que su análisis ha de hacerse desde el ámbito jurídico en el que nace y alcanza proyección, en otro caso, se correría el riesgo de distorsionar a priori el objeto de estudio, desvirtuándose así la comprensión de su extraordinaria repercusión para la cultura jurídica norteamericana, […][67]

Ahora bien, se puede apreciar que la parte del derecho a la intimidad y a la protección de datos personales, tienen puntos de contacto y conexión, pero un tanto diferentes en su desarrollo y aplicación; se podría entender que el derecho a la intimidad parte de interpretaciones a diferentes enmiendas tomando un tinte de derechos fundamentales; mientras que la protección de datos personales parte más de derechos de protección al consumidor.

En el Derecho a la Intimidad, Pablo Dermizaky comenta:

> La Constitución Estadounidense y sus Enmiendas no mencionan explícitamente el derecho a la intimidad que, sin embargo, ha sido reconocido por la Corte Suprema de ese país como implícito en la libertad personal de la Primera Enmienda y de la Enmienda XIV, en la reserva de derechos del pueblo que hace la Novena Enmienda, y en la Cuarta y Quinta Enmiendas.
>
> El concepto ha sido expuesto en los casos célebres resueltos por dicha Corte, como en el ya mencionado de las escuchas telefónicas, y en el del derecho al aborto de Roe Vs. Wade (1973), en el que el Justicie Douglas dijo que el derecho a la intimidad es anterior al *Bill of Rights*, «más antiguo que nuestros partidos políticos y que nuestro sistema escolar». Se refirió a tres niveles descendientes de derechos fundamentales: primero, el derecho de «control automático sobre la propia inteligencia y personalidad; segundo, la libertad de escoger en las cuestiones básicas sobre la propia vida, como el matrimonio, la procreación y la crianza de los hijos; y tercero, la libre elección de los medios para cuidar su persona y su salud. William Prosser, en su artículo «Privacy», publicado en el Nº 383 de la California Law Review (1960), enumera cuatro áreas en las que rige el derecho a la intimidad: l) contra la intrusión en la reclusión o soledad, o en los asuntos privados de uno; 2) contra la revelación de actos privados embarazosos; 3) contra la publicidad que coloca a uno en una falsa imagen ante el público; y 4) contra la apropiación

[67] Nieves Saldaña, María, *«The Right to Privacy» La génesis de la Protección de la Privacidad en el sistema constitucional norteamericano: El centenario legado de Warren y Brandeis*, España, Revista de Derecho Político, No. 85, 2012, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://doi.org/10.5944/rdp.85.2012.10723* pp. 199-203.

del nombre de uno en beneficio de otro.[68]

Por su parte, “El enfoque norteamericano sobre esta materia no considera la protección de datos como un derecho fundamental sino como un derecho del consumidor. Está integrado por algunas disposiciones sectoriales y no estima necesaria la existencia de las autoridades de control especializadas en tratamiento de datos personales sin perjuicio que tengan otras formas de control. Prefieren la autorregulación y la promulgación de varias normas sectoriales en lugar de disposiciones generales. Así, por ejemplo, se han expedido, entre otras, las siguientes normas federales:”[69]

- *The Fair Credit Reporting Act of 1970 (FCRA);*
- *Bank Secrecy Act of 1970;*
- *Privacy Act of 1974;*
- *Family Educational Rights and Privacy Act of 1974;*
- *Right to Financial Privacy Act of 1978*
- *Foreign Intelligence Surveillance Act of 1978*
- *Privacy Protection Act of 1980*
- *Cable Communications Policy Act of 1984*
- *Electronic Communications Privacy Act of 1986 (ECPA);*
- *Computer Matching and Privacy Protection Act of 1988*
- *Employee Polygraph Protection Act of 1988*
- *Video Privacy Protection Act of 1988*
- *Telephone Consumer Protection Act of 1991*
- *Driver´s Privacy Protection Act of 1994*
- *Communications Assistance for Law Enforcement Act of 1994*
- *Personal Responsibility and Work Opportunity Reconciliation Act of 1996*
- *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*
- *The Consumer Credit Reporting Reform Act of 1996*
- *Identity Theft and Assumption Deterrence Act of 1998*
- *Children´s Online Privacy Protection Act of 1998*
- *Gramm-Leach-Bliley Act of 1999*
- *USA Patriot Act of 2001*
- *The Confidential Information Protection and Statistical Act of 2002*
- *The Federal Information Security Management Act of 2002*
- *CAN-SPAM Act of 2003*
- *Video Voyeurism Prevention Act of 2004*

[68] Dermizaky Peredo, Pablo, *El derecho a la Intimidad*, *op. cit.* pp 180-181.
[69] INAI, *Introducción y antecedentes del Derecho a la Protección de Datos Personales*, [en línea] México, INAI, 2015, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *http://metabase.uaem.mx/xmlui/bitstream/handle/123456789/2523/1%20Introduccio%CC%81n%20y%20antecedentes%20del%20Derecho%20a%20la%20Proteccio%CC%81n%20de%20Datos%20Personales.pdf?sequence=1&isAllowed=y* pp. 18-19.

1.2.1.1 Habeas Data

La Maestra Alba Medrano nos menciona con respecto al habeas data lo siguiente:

> La raíz etimológica de ambas voces utilizadas (habeas y data) es más precisamente explicada por Cretella Júnior, quien menciona "análogamente al *habeas corpus*, la expresión *habeas data* es formada del vocablo *habeas* y *data*, acusativo neutro plural de *datum*, de la misma raíz que el verbo latino *do, das, dedi, datum, dare,* igual a "dar", #ofrecer". *Datum* singular de *data* es empleado por Propercio, en las Elegías libro III, Elegía 15, verso 6: "*nullis capata Lycina datis*" y por Ovidio, en las *Metamorfosis*, libro VI, verso 363, ambos con el sentido de "presentes", "donativos", "ofertas", y no con el sentido de "datos". Los diccionarios de la lengua inglesa traducen "*datum",* plural *"data*", por "*facts*", "*things certainly known*"; "*no or avaible*". En portugués, el *data* es traducido por "documentos"", "datos" (común en el lenguaje de la informática: procesamiento de datos). "Datos" son "informaciones", que constan en archivos, en bancos de datos. "Informaciones relativas a las personas, que constan en registros o bancos son datos. Así, *habeas data* al pie de la letra significa: "toma los datos que están en tu poder y entrégalos al interesado" o "brinda al interesado, mediante certificación, todos los datos o documentos que se encuentran en tu poder que pueda defender él sus derechos en juicio" (Puccinelli, p.296)[70]

Para esta autora el *habeas data* es un "recurso procesal diseñado para controlar la información personal contenida en bancos de datos, cuyo derecho implica la corrección, la cancelación, y la posibilidad de restringir y limitar la circulación de los mismos." De esta manera, "adoptado este concepto por diversos países latinoamericanos simulando el recurso del *habeas corpus* que protege la libertad, el *habeas data* protege la información nominativa, es decir, aquella que identifica al individuo."[71]

Ahora bien, según Néstor Sagüés "el *habeas data* es un proceso constitucional con fines diversos. Literalmente, apunta a "traer los datos" (así como el hábeas corpus «sic» procura "traer el cuerpo"), y su objetivo principal es contener ciertos excesos del llamado "poder informático".

> Como tal, el *habeas data* genera dos órdenes de interrogantes. El primero es típicamente de derecho constitucional: ¿cuáles son los derechos en juego (y en conflicto) en el *habeas data*? ¿qué categoría de derechos debe privilegias el legislador y el juez en el habeas data? La segunda esfera de problemas es propia del derecho procesal constitucional: ¿qué trámite tiene que darse al hábeas data «sic»? ¿quién debe tener legitimación activa y pasiva? ¿cuál será el órgano competente para conocer y decidir en él?[72]

[70] Muñoz de Alba Medrano, Marcia, *Habeas Data*, en "Documentos de trabajo del Instituto de Investigaciones Jurídicas. 2001", [en línea] México, UNAM-IIJ, 2001, [fecha de consulta: 3 de diciembre de 2022] Disponible en:https://archivos.juridicas.unam.mx/www/bjv/libros/10/4643/11.pdf p. 1.

[71] *Idem*.

[72] Sagüés, Néstor Pedro, *El Habeas Data: Su desarrollo constitucional*, en "V Congreso

Sagüés, sostiene que el *habeas data* está relacionado con el derecho informático, así como por el poder informático: en este sentido, vale la pena hacer un breve paréntesis para tener en cuenta que el denominado derecho informático en palabras de Julio Téllez es "una rama de las ciencias jurídicas que contempla a la informática como instrumento (informática jurídica) y como objeto de estudio (derecho de la informática). En función de lo anterior, es notorio que la clasificación del dicho Derecho Informático obedecerá a dos vertientes fundamentales: la informática jurídica y el derecho de la informática". [73]

Regresando con Sagüés, el derecho informático, pero sobre todo el denominado poder informático puede entrar en colisión con los derechos constitucionales de las personas registradas en diferentes bases de datos que podrían ser de índole público o privado.

> Al cotejar el *habeas corpus* y el *habeas data* se comprueba una inicial coincidencia en lo referente a su naturaleza jurídica. En ambos casos no se trata de derechos fundamentales, *stricto sensu*, sino de instrumentos o garantías procesales de defensa de los derechos a la libertad personal, en el caso del *habeas data*. Tanto el *habeas corpus* como el *habeas data* representan dos garantías procesales de aspectos diferentes de la libertad. Mientras el primero se circunscribe a la dimensión física y externa de la libertad; el segundo tiende a proteger prioritariamente aspectos internos de la libertad: la identidad de la persona, su autodeterminación, su intimidad.[74]

Existen diferentes tipos de *habeas data*, Sagüés los distingue de la siguiente manera:[75]

Tipo de *habeas data*	Características	Países del sistema Americano que lo tienen.
Informativo	Se utiliza para obtener la información nominativa determinada	Argentina, Brasil, Colombia, Ecuador, Guatemala, Paraguay y Perú
Aditivo	Actualizar o incluir datos o información dentro de los archivos	Argentina, Brasil, Colombia, Ecuador y Paraguay

Iberoamericano de derecho constitucional", [en línea] México, Estudios Doctrinales, Serie G., número 193, UNAM-IIJ, 1998, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://archivos.juridicas.unam.mx/www/bjv/libros/1/113/39.pdf* p. 859.

[73] Téllez Valdés, Julio, *Derecho Informático*, 2ª ed., México, McGraw-Hill, 1996, p. 22.

[74] Muñoz de Alba Medrano, Marcia, *Los nuevos derechos humanos en la era tecnológica: "¿El Habeas Data… La solución?"*, [en línea] en "V Congreso Iberoamericano de derecho constitucional", México, Estudios Doctrinales, Serie G., número 193, UNAM-IIJ, 1998, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://archivos.juridicas.unam.mx/www/bjv/libros/1/113/28.pdf* p. 593

[75] Sagüés citado por Muñoz de Alba Medrano, Marcia, *op.* cit. Nota. 69. p. 3.

Tipo de *habeas data*	Características	Países del sistema Americano que lo tienen.
Rectificador o Correctivo	Corregir informaciones falsas, inexactas o imprecisas	Argentina, Brasil, Colombia, Ecuador, Guatemala y Paraguay
Reservador	Asegurar que un dato determinado sea proporcionado a quienes se encuentran legalmente autorizados para conocerlo	s/d
Exclutorio o cancelatorio	Trata de eliminar información almacenada en algún banco de datos o sistema de información, tiene relevancia para aquella información considerada como sensible	Argentina, Ecuador, y Paraguay

Importante destacar también los alcances, así como la compatibilidad entre el Derecho Informático y el *habeas data* siendo tales:

1) Derecho al Acceso: Qué información se tiene de una persona.
2) Derecho a la actualización: Poner al día los datos personales.
3) Derecho a la rectificación: Corrección de información inexacta.
4) Derecho a la confidencialidad: Secrecía de información para con terceros
5) Derecho a la exclusión: Cancelar datos.[76]

No obstante, perece que este derecho de *habeas data* al ser de una naturaleza más procesal, se debe tener en cuenta que al juicio del que esto escribe, tanto el derecho a la protección de datos personales, como el derecho de acceso a la información, son dos derechos que están íntimamente ligados y que en México forman parte de la llamada tercera generación de derechos humanos; por ello es mejor hablar más de protección de datos personales y autodeterminación informativa, mejor que de habeas data.

En este sentido, la jueza Jenny Quirós de Costa Rica indica que “el hábeas data podría referirse a una construcción conceptual para englobar todos aquellos elementos sustantivos y procedimentales creados para la protección de la persona frente al tratamiento de sus datos personales.”[77]

[76] *Cfr.* Sagüés, Néstor Pedro, *op. cit.* Nota 71, p. 862.
[77] Quirós Camacho, Jenny, *La Protección de Datos Personales y el habeas data. Elementos para iniciar una discusión en Costa Rica*, en “Revista de Ciencias Jurídicas”, Costa Rica, Portal de Revistas Académicas, número 103, 2004, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://revistas.ucr.ac.cr/index.php/juridicas/article/download/13370/14345/* p. 153

> Las diferencias apuntadas entre el amplio espectro de la protección de datos y el hábeas data entendido como garantía procesal, ha llevado a algunos a establecer entre ambos una relación de género a especie: "Existe una relación de género y especie entre el hábeas data y el derecho de acceso a la información, como derechos humanos referidos a la accesibilidad de datos. El derecho de acceso a la información interpreta una necesidad general, mientras que el habeas data se vincula a una necesidad especial y personal, siendo ambos incuestionables, pero dedicados a espectros y casos diferentes."
>
> Lo importante en nuestro criterio es que junto a la garantía procesal se prevea para la verdadera protección del ciudadano, el derecho a la información sobre las formas en que se realizaría el tratamiento de los datos, los objetivos del mismo y su destino final, a efecto de que la persona esté o pueda estar en condiciones de conocer que sus datos serán objeto de manejos más allá de su voluntad, y poder evitarlo. Es por ello que acogemos la afirmación de que hablar de hábeas data no es suficiente, y que es preferible referirse a la necesidad humana de protección de los datos personales, misma que tiene como correlativo bien jurídico la autodeterminación informativa.[78]

1.2.2 En México

La protección de los datos personales en México se puede dividir en dos grandes momentos. En primer lugar, la protección de Datos Federales al amparo de la primer Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental que data del 2002.

En este primer momento es de señalar que se presentan las dos reformas constitucionales claves en la historia de los datos personales en México; siendo la primera del 20 de julio de 2007, donde se contemplaron limitantes al ejercicio del derecho a la información según la reforma al artículo 6° constitucional en sus fracciones I y II. A continuación, la reforma constitucional del 01 de junio de 2009, donde se plasmó en el artículo 16 como derecho humano la protección de los datos personales, así como los llamados derechos ARCO.

El segundo momento considero que se inicia con la reforma constitucional del 30 de abril de 2009; la cual adiciona la fracción XXIX-O del artículo 73 constitucional, en donde se establece como facultad exclusiva del Congreso de la Unión, la de legislar en materia de protección de datos personales en posesión de particulares.

Por lo anterior este punto lo abordaré tomado en consideración estos dos momentos:

[78] *Ibidem*. pp. 153-154.

1.2.2.1 Historia en México de la Protección de Datos Personales en Posesión de Sujetos Obligados.

La protección de los datos personales está íntimamente ligada con el acceso a la información y la protección de archivos. Si bien es cierto que con la llamada reforma política de los 70's se inició con la incipiente protección al derecho a la información no fue sino hasta el cambio político del 2000, que la protección de datos personales cobró mayor relevancia.

Y no fue sino con la expedición de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental -en adelante LFTAIPG- en 2002 que se reservó un capítulo especial para la protección de Datos Personales. Para cuestiones del presente trabajo la parte histórica de esta Ley se quedará reservada para la parte correspondiente.

Cabe señalar de forma preliminar, que al momento de expedición de la LFTAIPG la protección de datos personales estaba únicamente relacionada al sector de los llamados sujetos obligados que en aquel momento obligaba a los Poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal, y cualquier otra entidad federal de acuerdo con lo dispuesto por el artículo primero de dicha ley.

Ya fue hasta 2010, y derivado de diferentes reformas constitucionales que se mencionarán más adelante, fue necesario abarcar el ámbito de protección de datos personales en posesión de particulares.

La LFTAIPG definió a los Datos Personales en el artículo 3 fracción II, la cual sufrió una modificación antes de ser abrogada:

Original DOF 11/06/2002	Modificación DOF 05/07/2010
Artículo 3.- Para los efectos de esta Ley se entenderá por: […] II. Datos personales: La información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad.	Artículo 3.- Para los efectos de esta Ley se entenderá por: I. ... II. Datos personales: Cualquier información concerniente a una persona física identificada o identificable.

La modificación a la definición de datos personales en 2010 ocurrió el mismo día que fue publicada la Ley Federal de Protección de Datos Personales en Posesión de Particulares -en adelante LFPDPPP-, con el fin de homologar en un solo género, la definición de Datos Personales en ambas legislaciones, tal como se puede apreciar en el siguiente cuadro:

Nueva definición de Datos Personales en LFTAIPG DOF 05/07/2010	Definición de Datos Personales en LFPDPPP DOF 05/07/2010
Artículo 3.- Para los efectos de esta Ley se entenderá por: I. ... II. Datos personales: Cualquier información concerniente a una persona física identificada o identificable;	Artículo 3.- Para los efectos de esta Ley se entenderá por: I. ... II. … III. … IV. … V. Datos personales: Cualquier información concerniente a una persona física identificada o identificable.

Por su parte el capítulo IV (cuarto) de esta ley fue destinado a la protección de datos personales de los artículos 20 al 26. A su vez el Reglamento de la LFTAIPG en su capítulo VIII (Octavo) hace solamente una mención a la protección de datos personales en sus artículos 47 y 48.

De una manera que se podría decir incipiente tanto la LFTAIPG como su Reglamento, apenas indicaban cómo realizar el tratamiento de los datos personales, así como el procedimiento de derechos de acceso, rectificación, cancelación y oposición de datos personales (derechos ARCO). La entonces LFTAIPG reguló la parte de datos personales de la siguiente manera:

> Capítulo IV Protección de datos personales
>
> Artículo 20. Los sujetos obligados serán responsables de los datos personales y, en relación con éstos, deberán:
>
> I. Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos, así como capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos, de conformidad con los lineamientos que al respecto establezca el Instituto o las instancias equivalentes previstas en el Artículo 61;
>
> II. Tratar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

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

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

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

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

Artículo 21. Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información.

Artículo 22. No se requerirá el consentimiento de los individuos para proporcionar los datos personales en los siguientes casos:

I. Los necesarios para la prevención o el diagnóstico médico, la prestación de asistencia médica o la gestión de servicios de salud y no pueda recabarse su autorización; [FRACCIÓN DEROGADA DOF: 11/05/2004]

II. Los necesarios por razones estadísticas, científicas o de interés general previstas en ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran;

III. Cuando se transmitan entre sujetos obligados o entre dependencias y entidades, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos;

IV. Cuando exista una orden judicial;

V. A terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquéllos para los cuales se les hubieren transmitido, y

VI. En los demás casos que establezcan las leyes.

Artículo 23. Los sujetos obligados que posean, por cualquier título, sistemas de datos personales, deberán hacerlo del conocimiento del Instituto o de las instancias equivalentes previstas en el Artículo 61, quienes mantendrán un listado actualizado de los sistemas de datos personales.

Artículo 24. Sin perjuicio de lo que dispongan otras leyes, 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. Aquélla deberá entregarle, en un plazo de diez días hábiles contados desde la presentación de la solicitud, en formato comprensible para el solicitante, la información correspondiente, o bien, le comunicará por escrito que ese sistema de datos personales no contiene los referidos al solicitante.

La entrega de los datos personales será gratuita, debiendo cubrir el individuo únicamente los gastos de envío de conformidad con las tarifas aplicables. No obstante, si la misma persona realiza una nueva solicitud respecto del mismo sistema de datos personales en un periodo menor a doce meses a partir de la última solicitud, los costos se determinarán de acuerdo con lo establecido en el Artículo 27.

Artículo 25. 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. Con tal propósito, el interesado deberá entregar una solicitud de modificaciones a la unidad de enlace o su equivalente, que señale el sistema de datos personales, indique las modificaciones por realizarse y aporte la documentación que motive su petición. Aquélla deberá entregar al solicitante, en un plazo de 30 días hábiles desde la presentación de la solicitud, una comunicación que haga constar las modificaciones o bien, le informe de manera fundada y motivada, las razones por las cuales no procedieron las modificaciones.

Artículo 26. Contra la negativa de entregar o corregir datos personales, procederá la interposición del recurso a que se refiere el Artículo 50. También procederá en el caso de falta de respuesta en los plazos a que se refieren los artículos 24 y 25.

Por su parte el Reglamento de la entonces LFTAIPG reglamentaba la parte de datos personales de la siguiente forma:

Capítulo VIII
Protección de datos personales

Artículo 47. Los procedimientos para acceder a los datos personales que estén en posesión de las dependencias y entidades garantizarán la protección de los derechos de los individuos, en particular, a la vida privada y a la intimidad, así como al acceso y corrección de sus datos personales, de conformidad con los lineamientos que expida el Instituto y demás disposiciones aplicables para el manejo, mantenimiento, seguridad y protección de los datos personales.

Artículo 48. Las dependencias y entidades que cuenten con sistemas de datos personales deberán hacer del conocimiento del Instituto y del público en general a través de sus sitios de internet, el listado de dichos sistemas, en el

cual indicarán el objeto del sistema, el tipo de datos que contiene, el uso que se les da, la unidad administrativa que lo administra y el nombre del responsable. El Instituto mantendrá un listado público actualizado de los sistemas de datos personales que sean hechos de su conocimiento.

Con la entrada en vigor de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental se estableció en su artículo Octavo Transitorio, que los particulares podrían presentar las solicitudes de acceso a la información, a los datos personales y a la corrección de éstos un año después. En función de ello se emitieron una serie de lineamientos y avisos; así como sus respectivas modificaciones a los mismos donde se referían tanto a la parte de transparencia y acceso a la información, como a la parte de datos personales. De forma esquemática dichos lineamientos y avisos fueron los siguientes:

FECHA DE PUBLICACIÓN DOF	NOMBRE DE LA DISPOSICIÓN
12/06/2003	LINEAMIENTOS que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento y trámite de las solicitudes de acceso a la información gubernamental que formulen los particulares, así como en su resolución y notificación, y la entrega de la información en su caso, con exclusión de las solicitudes de acceso a datos personales y su corrección.
12/06/2003	AVISO por el que se dan a conocer los formatos de solicitudes de acceso a la información, de acceso y corrección a datos personales, y de recurso de revisión, cuya presentación no se realiza a través de medios electrónicos.
25/08/2003	LINEAMIENTOS que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de acceso a datos personales que formulen los particulares, con exclusión de las solicitudes de corrección de dichos datos.
30/09/2005	LINEAMIENTOS de Protección de Datos Personales.
02/12/2008	MODIFICACIONES a los Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento y trámite de las solicitudes de acceso a la información gubernamental que formulen los particulares, así como en su resolución y notificación, y la entrega de la información en su caso, con exclusión de las solicitudes de acceso a datos personales y su corrección; Lineamientos que deberán observar las dependencias y entidades de la

FECHA DE PUBLICACIÓN DOF	NOMBRE DE LA DISPOSICIÓN
	Administración Pública Federal en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de acceso a datos personales que formulen los particulares, con exclusión de las solicitudes de corrección de dichos datos, y Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal, en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de corrección de datos personales que formulen los particulares.

De la lista de Avisos y Lineamientos arriba mencionados los Lineamientos de Protección de Datos Personales de 2005, constituyeron el primer marco normativo que detalla las diferentes formas de tratamiento de datos personales. En cuanto al objeto y ámbito de aplicación tenemos los siguiente:

> Objeto y ámbito de aplicación
>
> Primero. Los presentes Lineamientos tienen por objeto establecer las políticas generales y procedimientos que deberán observar las dependencias y entidades de la Administración Pública Federal para garantizar a la persona la facultad de decisión sobre el uso y destino de sus datos personales, con el propósito de asegurar su adecuado tratamiento e impedir su transmisión ilícita y lesiva para la dignidad y derechos del afectado.
>
> Para tal efecto, este ordenamiento establece las condiciones y requisitos mínimos para el debido manejo y custodia de los sistemas

Estos lineamientos regularon lo siguiente:

i) Principios de la protección de datos personales
ii) Calidad de Datos
iii) Tratamiento de los Datos personales
iv) Conservación de datos personales
v) Transmisión de datos personales
vi) Consentimiento del titular de los datos personales
vii) Seguridad de los Sistemas de Datos Personales

Cabe señalar que, en el caso de las entidades federativas, no todas tuvieron una ley de protección de datos personales, algunas mantuvieron una estructura similar a la federal en el sentido de que los datos personales quedaron protegidos en las leyes de transparencia y acceso a la información pública de cada entidad federativa.

Sirva el presente cuadro:

Entidad Federativa	Ley	Fecha de Publicación
Aguascalientes	Ley de Transparencia y Acceso a la Información Pública del Estado de Aguascalientes	22 de mayo de 2006
Baja California	Ley de Acceso a la Información Pública para el Estado de Baja California Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California	12 de Agosto de 2005 01 de octubre de 2010
Baja California Sur	Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California Sur	12 de marzo de 2010
Campeche	Ley de Protección de Datos Personales del Estado de Campeche y sus Municipios	09 de julio de 2012
Ciudad de México	Ley de Protección de Datos Personales para el Distrito Federal	03 de octubre de 2008
Coahuila de Zaragoza	Ley de Acceso a la Información Pública y Protección de Datos Personales para el Estado de Coahuila de Zaragoza	02 de septiembre de 2008
Colima	Ley de Protección de Datos Personales del Estado de Colima	21 de junio de 2003
Durango	Ley de Transparencia y Acceso a la Información Pública del Estado de Durango	11 de julio de 2008
Estado de México	Ley de Protección de Datos Personales del Estado de México	31 de agosto de 2012
Guanajuato	Ley de Protección de Datos Personales para el Estado y Municipios de Guanajuato	19 de mayo de 2006
Guerrero	Ley Número 374 de Transparencia y Acceso a la Información Pública del Estado de Guerrero	15 de junio de 2010
Hidalgo	Ley de Transparencia y Acceso a la Información Pública Gubernamental para el Estado de Hidalgo	29 de diciembre de 2006
Jalisco	Ley de Información Pública del Estado de Jalisco y sus Municipios	22 de diciembre de 2012
Michoacán	Ley de Transparencia y Acceso a la Información Pública del Estado de Michoacán de Ocampo	07 de noviembre de 2008

Entidad Federativa	Ley	Fecha de Publicación
Morelos	Ley de Información Pública, Estadística y Protección de Datos Personales del Estado de Morelos	27 de agosto de 2003
Nayarit	Ley de Transparencia y Acceso a la Información Pública del Estado de Nayarit	16 de junio de 2004
Nuevo León	Ley de Transparencia y Acceso a la Información del Estado de Nuevo León	19 de julio de 2008
Oaxaca	Ley de Protección de Datos Personales del Estado de Oaxaca	23 de agosto de 2008
Puebla	Ley de Protección de Datos Personales del Estado de Puebla	25 de noviembre del 2013
Querétaro	Ley de Acceso a la Información Gubernamental del Estado de Querétaro	27 de septiembre de 2002
Quintana Roo	Ley de Transparencia y Acceso a la Información Pública del Estado de Quintana Roo	31 de mayo de 2004
San Luis Potosí	Ley de Transparencia y Acceso a la Información Pública del Estado de San Luis Potosí	18 de octubre de 2007
Sinaloa	Ley de Acceso a la Información Pública del Estado de Sinaloa	26 de abril de 2002
Sonora	Ley de Acceso a la Información Pública y de Protección de Datos Personales del Estado de Sonora	25 de febrero de 2005
Tabasco	Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco	10 de febrero de 2007
Tamaulipas	Ley de Transparencia y Acceso a la Información Pública del Estado de Tamaulipas	05 de julio de 2007
Tlaxcala	Ley de Protección de Datos Personales para el Estado de Tlaxcala	14 de mayo de 2012
Veracruz	Ley para la Tutela de los Datos Personales en el Estado de Veracruz de Ignacio de la Llave	02 de octubre de 2012
Yucatán	Ley de Acceso a la Información Pública para el Estado y los Municipios de Yucatán	31 de mayo de 2004
Zacatecas	Ley de Transparencia y Acceso a la Información Pública del Estado de Zacatecas	29 de junio de 2011

El 20 de julio de 2007, se publicó en el Diario Oficial de la Federación el Decreto por el que se adiciona un segundo párrafo con siete fracciones al Artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos. En dicho párrafo en su fracción segunda quedó plasmada con rango constitucional, la protección de datos personales atendiendo a la parte de sujetos obligados de la siguiente manera:

> Artículo 6o.- ...
>
> 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.

Por su parte, en el Plan Nacional de Desarrollo 2007-2012 la parte de la protección de datos personales en sujetos obligados se manifestó lo siguiente:

> 5.5 Transparencia y rendición de cuentas […]
>
> La publicación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental el 11 de junio de 2002, permitió contar con un marco regulatorio para el acceso a la información del Gobierno Federal. Con la promulgación de esta ley, se cubrió un profundo vacío legal e institucional, ya que ahora cualquier persona puede solicitar información del Gobierno Federal. Asimismo, se asegura la transparencia y la rendición de cuentas en el Gobierno Federal, porque se obliga a contar con procedimientos sencillos y expeditos en materia de acceso a la información; se garantiza la protección de los datos personales en posesión de los sujetos obligados y se establece la obligación de contar con archivos bien ordenados.[…]
>
> OBJETIVO 5
> Promover y garantizar la transparencia, la rendición de cuentas, el acceso a la información y la protección de los datos personales en todos los ámbitos de gobierno.
>
> Para lograr este objetivo se implementarán las siguientes estrategias:
>
> ESTRATEGIA 5.2 Fortalecer a los organismos encargados de facilitar el acceso a la información pública gubernamental y de proteger los datos personales.
>
> Es necesario que en las distintas esferas de gobierno se establezcan mecanismos de acceso a la información y procedimientos de revisión expeditos. En este último caso es necesario contar con órganos u organismos especializados e imparciales con autonomía operativa, de gestión presupuestaria y de decisión.

La siguiente modificación constitucional importante en el tema de datos personales de sujetos obligados fue el 07 de febrero de 2014 al artículo 73 en la cual quedó

plasmada de la siguiente forma:

> Artículo 73. ...
>
> XXIX-S. Para expedir las 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 niveles de gobierno.

Posteriormente a esta reforma constitucional de 2014, se presenta en 2015 una iniciativa de ley para regular de forma particular y de manera general la protección de datos personales en posesión de sujetos obligados.

Dicha iniciativa reconoce lo siguiente:

> Conjuntamente con la reforma al citado artículo 16 constitucional, se adiciona la fracción XXIX-O del artículo 73, en donde se establece como facultad exclusiva del Congreso de la Unión, legislar en materia de protección de datos personales en posesión de los particulares. Con ello, esta materia se constituye como materia federal, no concurrente, por lo que las entidades federativas no cuentan con facultades para legislar al respecto.
>
> Así, en 2010 se expidió la Ley Federal de Protección de Datos Personales en Posesión de los Particulares cuyo objeto es la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. Esta ley encomendó al Instituto Federal de Acceso a la Información y Protección de Datos constituirse en el garante de este derecho.
>
> No obstante, el avance de la materia con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, la reciente reforma de 2014 en materia de transparencia reconoce la necesidad de abundar en el derecho de protección de datos personales en posesión de sujetos obligados.
>
> El marco jurídico de la protección de datos en posesión de sujetos obligados ha resultado insuficiente. […]
>
> No resulta menor, por tanto, esta posibilidad histórica que brinda el constituyente permanente de dotar a los habitantes del territorio mexicano de una ley general de protección de datos personales para el ámbito público, que desarrolle sustantivamente este derecho a partir de los principios, deberes y derechos que internacionalmente han sido reconocidos, de manera que la protección de datos personales se vea emancipada del derecho de acceso a la información, y en ese sentido deje de visualizársele como un accesorio de ese derecho. A partir de esta consideración, el derecho a la protección de datos deberá considerarse en un esquema de igualdad con el acceso a la información y el resto de los derechos fundamentales que establece nuestra Carta Magna.

> La reforma en materia de transparencia, sin duda marcó un hito en el desarrollo del derecho a la protección de datos en México, ya que a través de la misma se establecen las bases constitucionales para dotar al sector público federal de un régimen legal en materia de protección de datos, más aun, se abre la posibilidad de que se emita una ley general en la que se establezcan los principios, bases y procedimientos que de manera uniforme regule este derecho en nuestro país en los tres niveles de gobierno.
>
> Estas modificaciones constitucionales poseen un matiz histórico en materia de datos personales, pues, por una parte, dota al IFAI de autonomía constitucional y lo sitúa como el máximo órgano garante en materia de protección de datos personales en el ámbito público federal y, por otra, fija las bases para la creación de una ley general de protección de datos personales que permitirá dimensionar, en una situación sin precedentes, en toda su extensión el derecho a la protección de datos personales entre los entes públicos de los tres órdenes de gobierno.[…]
>
> Con esta propuesta, se busca que México dote a sus habitantes de leyes de vanguardia en el espacio de los derechos fundamentales con el objeto de proveerles de herramientas jurídicas que les permitan imponer un límite a las actuaciones de las autoridades que pudieran conculcar la esfera de derechos de los particulares. En este caso específico, un límite para ejercer de manera plena el derecho a la autodeterminación informativa de manera que cada persona en este país decida libremente sobre el uso y destino de sus datos personales, teniendo en todo momento el derecho a acceder, rectificar, cancelar y oponerse legítimamente a determinados tratamientos de datos.
>
> En ese orden de ideas, resulta conveniente que las leyes de acceso a la información prevean un apartado de protección de datos personales, para fijar los límites del acceso a la información frente a los datos personales, así como para establecer procedimientos y garantías para los casos de apertura de datos por considerarse de interés público, también lo es que el contenido sustantivo del derecho de protección de datos personales tanto el constitucional, como el que deviene de los tratados internacionales en materia de derechos humanos, de acuerdo al artículo 1 constitucional, sea desarrollado por leyes específicas y especializadas en materia de protección de datos personales.
>
> Bajo la concepción antes descrita es que el presente proyecto ha desarrollado, una ley general de protección de datos personales que de manera independiente y autónoma a cualquier otro derecho, empodere a los titulares del derecho frente al Estado Mexicano para garantizar el control sobre su información personal.[79]

Derivado de esta iniciativa, el pasado 26 de enero de 2017 se publicó la actual Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados que

[79] Cámara de Senadores, *Iniciativa con proyecto de decreto por la que se expide la ley general de protección de datos personales en posesión de sujetos obligados*, [en línea] s/d. [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.senado.gob.mx/comisiones/gobernacion/docs/proteccion_datos/Iniciativa.pdf* pp. 3 a 6.

actualmente nos rige.

Asimismo, el pasado 26 de enero de 2018 se emitió el Acuerdo mediante el cual se aprueban los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Por último, veamos las leyes estatales en materia de protección de datos personales a nivel estatal.

Entidad Federativa	Ley	Fecha de Publicación
Aguascalientes	Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Aguascalientes y sus Municipios	3 de julio de 2017
Baja California	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California	18 de Agosto de 2017
Baja California Sur	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California Sur	17 de julio de 2017
Campeche	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche	26 de julio de 2017
Ciudad de México	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México	10 de abril de 2018
Coahuila de Zaragoza	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Coahuila de Zaragoza	21 de julio de 2017
Colima	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Colima	09 de septiembre de 2017
Durango	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Durango	11 de junio de 2017
Estado de México	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios	30 de mayo de 2017
Guanajuato	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Guanajuato	14 de julio de 2017
Guerrero	Ley número 466 de Protección de Datos Personales en Posesión de Sujetos Obligados de Estado de Guerrero	18 de julio de 2017

Entidad Federativa	Ley	Fecha de Publicación
Hidalgo	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo	24 de julio de 2017
Jalisco	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios	26 de julio de 2017
Michoacán	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo	13 de noviembre de 2017
Morelos	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Morelos	26 de julio de 2017
Nayarit	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Nayarit	21 de octubre de 2017
Nuevo León	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León	11 de diciembre de 2019
Oaxaca	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Oaxaca	29 de noviembre de 2017
Puebla	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla	26 de julio de 2017
Querétaro	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Querétaro	26 de enero de 2018
Quintana Roo	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Quintana Roo	04 de julio de 2017
San Luis Potosí	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de San Luis Potosí	17 de diciembre de 2017
Sinaloa	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Sinaloa	26 de julio de 2017
Sonora	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Sonora	13 de octubre de 2017
Tabasco	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco	09 de septiembre de 2017
Tamaulipas	Ley de Protección de Datos Personales	17 de agosto de

Entidad Federativa	Ley	Fecha de Publicación
	en Posesión de Sujetos Obligados del Estado de Tamaulipas	2017
Tlaxcala	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tlaxcala	18 de julio de 2017
Veracruz	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Veracruz de Ignacio de la Llave	27 de julio de 2017
Yucatán	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Yucatán	17 de julio de 2017
Zacatecas	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Zacatecas	15 de julio de 2017

1.2.2.2 Historia en México de la Protección de Datos Personales en Posesión de Particulares

Se puede considerar al Plan Nacional de Desarrollo 2007-2009 publicado en el Diario Oficial de la Federación el 31 de mayo de 2007, como el primer antecedente para la protección de datos personales en posesión de particulares; cabe mencionar como se señaló en el inciso a) anterior, que también en este Plan se mencionaron diferentes aspectos respecto a la regulación de datos personales en posesión de sujetos obligados.

La estrategia 5.3 dispuso lo siguiente:

> ESTRATEGIA 5.3 Desarrollar el marco normativo que garantice que la información referente a la vida privada y a los datos personales estará protegida.
>
> La Ley Federal de Transparencia garantiza la protección de los datos personales en posesión de los sujetos obligados en el ámbito gubernamental. No obstante, es necesario el desarrollo de una Ley Federal en la materia que regule también aquéllos que se encuentran en poder de los particulares. Dicha regulación deberá incluir los principios de protección de datos personales reconocidos por los tratados internacionales en la materia, que el Estado mexicano debe observar.

Para ir acorde con este Plan, en 2007 se suscribieron iniciativas suscritas por el grupo parlamentario del PAN al artículo 73 constitucional para adicionar la parte correspondiente a la protección de datos personales en posesión de particulares. Originalmente, la iniciativa al artículo 73 fracción XXIX, era para el inciso N, luego pasó al inciso Ñ, y finalmente derivó en el inciso O como quedó actualmente.

A continuación, se presentan diferentes fragmentos del proceso legislativo:

> INICIATIVA con proyecto de decreto que reforma el artículo 73 de la Constitución Política de los Estados Unidos Mexicanos. Presentada por el diputado Luis Gustavo Parra Noriega, a nombre propio y de diversos diputados del grupo parlamentario del PAN. Se turnó a la Comisión de Puntos Constitucionales. Gaceta Parlamentaria, 27 de marzo de 2007
>
> **Exposición de Motivos**
>
> Sin duda, la necesidad de intimidad es inherente a la persona, y se constituye en un valor fundamental del ser humano; ya que para que el hombre se desarrolle y geste su propia personalidad e identidad, es menester que goce de un área que comprenda diversos aspectos de su vida individual y familiar, que esté libre de la intromisión de extraños.
>
> No es posible concebir un estado de bienestar personal y, en consecuencia, de bien común en la sociedad en general, sin la protección y salvaguarda adecuada de los derechos fundamentales del ser humano.
>
> Así pues, debemos entender que todos los seres humanos tenemos una vida "privada" conformada por aquella parte de nuestra vida que no está consagrada a una actividad pública, y que por lo mismo no está destinada a trascender e impactar a la sociedad de manera directa, y en donde en principio tanto el Estado como los particulares, no deben tener acceso a ella, toda vez que las actividades que se desarrollan no son de su incumbencia, ni les afectan.
>
> Ciertamente el concepto de vida privada es muy difícil de definir con precisión, pues tiene connotaciones diversas dependiendo de la sociedad de que se trate, sus circunstancias particulares y la época o el periodo correspondiente.
>
> Sin embargo, dentro de esta esfera de vida privada, podemos considerar a las relaciones personales y familiares, afectivas y de filiación, las creencias y preferencias religiosas, convicciones personales, inclinaciones políticas, condiciones personales de salud, identidad y personalidad psicológica, inclinaciones sexuales, comunicaciones personales privadas por cualquier medio, incluso algunos llegan a incluir la situación financiera personal y familiar.
>
> Así las cosas, en los últimos años hemos visto el incremento de la tendencia de la regulación de la protección de la privacidad de la información. No es un hecho extraño, dado que la privacidad de los individuos es desde luego un derecho humano fundamental de la mayor importancia.
> La privacidad de las personas abarca, naturalmente, la de la información que las identifica, o que versa sobre sus características o preferencias. En términos generales, estos datos son los que suelen llamarse "personales", pues por su propia definición y naturaleza corresponden e identifican a su titular. […]

Razón precisamente por la cual, en las reformas al artículo 6° de la Constitución General en materia de acceso a la información, aprobadas recientemente por esta soberanía, se estableció la obligación de que los órganos legislativos de las entidades federativas, legislaran sobre la protección de los datos personales en poder de los entes públicos. Al respecto, la finalidad de la recolección y tratamiento de los datos personales por los órganos del Estado, responde a un interés público, para instrumentar mediante análisis estadísticos, mejores servicios públicos, políticas que incidan en bien de la sociedad, o como medios para brindar certeza en la realización de determinados actos jurídicos.[…]

En nuestro país, la protección de los datos personales es un derecho en construcción; no obstante, que en tratándose de privacidad, nuestra norma máxima en los artículos 7° y 16, hacen mención de ella, aunque desde una perspectiva de garantías jurídico-constitucionales que se tiene como gobernados frente al Estado. […]

Así las cosas, es indispensable crear una legislación que recoja efectivamente los principios contenidos en el Marco de Privacidad de APEC, que provea a nuestras disposiciones legales con la visión vanguardista propuesta por APEC.

En gran medida, el Marco de Privacidad de APEC ha sido el instrumento internacional de mayor importancia, que sienta el paradigma de modelo de legislación sobre privacidad en muchos sentidos.

Esto es así porque de la mano con los Lineamientos de la OCDE, el Marco de Privacidad de APEC vino a enunciar los principios de contenido legislativo que, a la fecha, orientan los principales cuerpos normativos del mundo en la materia (particularmente, aunque no de forma exclusiva, de la mayoría de los países miembros de la OCDE y APEC).

Consideraciones todas ellas, que nos inclinan a pensar la necesidad de que se dicte una legislación cuyo ámbito material de aplicación los sea precisamente la totalidad del territorio nacional.

Una legislación que no únicamente atienda las recomendaciones internacionales de los organismos de los que México es parte, y que hoy por hoy simplemente reflejan los paradigmas y las prácticas prevalecientes de la protección de la privacidad por el sector privado en el mundo, sino que salde la deuda pendiente de ensanchar el derecho a la privacidad, en bien de todos los mexicanos.

Razón por la cual, debe destacarse que es impostergable la responsabilidad de esta soberanía para legislar en materia de protección de la privacidad de los datos personales de los individuos, no sólo por tratarse de un tema de protección de derechos humanos y libertades fundamentales, sino porque tiene un origen y efectos esenciales sobre la economía nacional y el aseguramiento del comercio irrestricto entre las entidades federativas, y con la regulación del comercio con otros estados extranjeros.

Cabe señalar, que el Congreso de la Unión, en términos de nuestro esquema de división de competencias entre los órdenes de gobierno del Estado mexicano, no cuenta con facultades expresas para legislar sobre la materia, y a la fecha, el establecimiento de marcos legislativos diversos en materia de protección de datos personales, por parte de las entidades federativas, puede dispersar el esfuerzo estatal por tutelar los aspectos más sensibles de la información personal, en perjuicio de los titulares de los mismos, establecer condiciones que restrinjan el comercio entre las propias entidades federativas, y resultar contrarios a los lineamientos adoptados por los organismos internacionales de los cuales forma parte el Estado mexicano.

Por las razones expuestas en la presente iniciativa, de acuerdo con las exposiciones de motivos y diversa memoranda explicativa tanto de los Lineamientos de la OCDE como del Marco de Privacidad de APEC, ambas organizaciones de las cuales es parte los Estados Unidos Mexicanos, como por la propia naturaleza de la legislación que se propone, que tiene un efecto innegable en la ampliación de la tutela de un derecho fundamental, como lo es la protección de los datos personales, en posesión de particulares, y el beneficio que una legislación de carácter federal sobre la materia puede traer respecto del comercio interestatal, y desde luego sobre el comercio internacional, sometemos a consideración de ese honorable Pleno de la Cámara de Diputados la siguiente

Iniciativa con proyecto de decreto.

Artículo Único. Se adiciona el inciso N) a la fracción XXIX del artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, para quedar como sigue:

Artículo 73. El Congreso tiene facultad:

I. a XXVIII. ...
XXIX. a XXIX-M. ...
XXIX-N. Para legislar en materia de protección datos personales en posesión de particulares.
XXX ...

Posteriormente en el dictamen de la Comisión de Puntos Constitucionales, se emitió proyecto de decreto por el que se adiciona la fracción XXIX-Ñ al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos. Aprobado en lo general y en lo particular con 371 votos en pro y 0 en contra. Se turnó a la Cámara de Senadores para sus efectos constitucionales. Gaceta parlamentaria, 12 de septiembre de 2007. Discusión y votación, 20 de septiembre de 2007:

[…]
II. Valoración de la iniciativa

La iniciativa presentada por los diputados Gustavo Parra, Rogelio Carbajal Tejada, Dora Alicia Martínez Valero, Esmeralda Cárdenas Sánchez y Jesús de León Tello relativa a la inclusión de la fracción XXIX-Ñ al artículo 73

constitucional, tiene como finalidad otorgarle la facultad exclusiva al Congreso de la Unión de legislar en materia de protección de datos personales en posesión de los particulares, dado que éstos se utilizan en mayor medida para llevar a cabo transacciones comerciales y que dicha materia constituye una competencia exclusiva del ámbito federal en toda la República. Lo anterior evita la existencia de asimetrías en la observancia de este nuevo derecho fundamental, permitiendo que se tutele eficazmente al evitar la proliferación de regímenes legales para su ejercicio y la posible deslocalización de los agentes regulados. Así, es necesario construir un derecho que pueda ser ejercido en todo el territorio nacional del mismo modo y bajo las mismas condiciones para cualquier interesado, no importando el estado o municipio del país donde se encuentre el titular de los datos personales. Además de lo anterior, debe reconocerse que el tratamiento de datos personales a través de tecnologías de la información, hacen que los mismos puedan ser transferidos en cuestión de segundos no sólo a nivel nacional sino también internacional, de forma tal que únicamente un régimen jurídico federal puede aproximar principios y bases comunes para atender los problemas inherentes a la protección de datos personales.

Cabe mencionar que diversos países regulan la protección de datos en posesión de los particulares, emitiendo una sola legislación aplicable en todo su territorio, logrando la uniformidad en la aplicación de los principios que rigen la materia y la efectiva tutela del derecho. […]

Se debe recordar que México es miembro de la OCDE, lo cual lo obliga ante este organismo a cumplir con sus principios y es precisamente éste el que plantea la obligación de los países miembros de asumir un compromiso con la adopción de principios generales para la protección de datos personales. De aprobarse el presente proyecto de decreto, en el que se adiciona la fracción XXIX-Ñ al artículo 73, se otorgará la facultad al Congreso de la Unión de legislar en materia de datos personales en posesión de particulares, con lo cual se estaría cumpliendo con dicho principio establecido por la OCDE. Con ello nuestro país mandaría un mensaje a la comunidad internacional de su interés por respetar el derecho a la privacidad a la que tienen derecho los ciudadanos. Derecho a proteger su intimidad en tanto no menoscaben el bien común o el derecho de terceros, ante lo cual el Estado debe tener la oportunidad de defender a sus ciudadanos.

Por ello, esta Comisión dictaminadora considera la conveniencia de proponer ante esta soberanía la aprobación de la reforma al artículo 73 constitucional en materia de protección de datos personales.

Artículo Único. Se adiciona la fracción XXIX-Ñ al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, para quedar como sigue:

Artículo 73. El Congreso tiene facultad:
I. a XXIX-N. ...
XXIX-Ñ. Para legislar en materia de protección de datos personales en posesión de
particulares.

XXX. ...

Ya en la cámara de senadores, se presentó el dictamen de las Comisiones Unidas de Puntos Constitucionales; y de Estudios Legislativos, Segunda, con proyecto de decreto por el que se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos. Aprobado en lo general y en lo particular con 99 votos en pro y 0 en contra. Se turno a las Legislaturas de los Estados para los efectos de lo dispuesto en el artículo 135 constitucional. Diario de los Debates, 2 de diciembre de 2008. Discusión y votación, 4 de diciembre de 2008:

II. MATERIA DE LA MINUTA

La minuta proyecto de Decreto por el que se adiciona la fracción XXIX-Ñ al artículo 73 constitucional, establece la facultad expresa del Congreso para expedir leyes en materia de protección de datos personales en posesión de particulares, ya que éstos son utilizados principalmente para realizar transacciones comerciales, siendo ésta una competencia exclusiva del ámbito federal.

La reforma de la minuta de mérito evitará la existencia de asimetrías en la observancia de este nuevo derecho, permitiendo que se tutele eficazmente al evitar la dispersión de regímenes legales.

De esta suerte, se estima necesario construir un derecho que pueda ser ejercido en todo el país bajo las mismas condiciones y del mismo modo para cualquier interesado, sin importar el lugar donde se encuentre el titular de los datos personales.

Asimismo, la minuta se refiere al tratamiento de datos personales a través de tecnologías de la información, que en la actualidad hacen que los mismos puedan ser transferidos rápidamente tanto a nivel nacional como internacional, por lo que se considera que únicamente un régimen jurídico federal puede asegurar los principios y bases comunes para atender los problemas inherentes a la protección de datos personales.

III. CONSIDERACIONES

• Estas comisiones unidas consideran que la propuesta de la minuta enviada por la Colegisladora es loable, ya que luego de haber reconocido con la publicación de la reforma al artículo 6° constitucional, la necesidad de proteger a la persona y sus derechos y libertades fundamentales, a través de una regulación del tratamiento de datos personales en posesión de los entes públicos, resulta necesario tener mecanismos para proteger los datos personales en posesión de personas privadas.

Así, la propuesta de reforma de la minuta en estudio se refiere a la facultad exclusiva del Congreso de la Unión para legislar en materia de protección de datos personales en posesión de particulares. […]

Según se desprende de las referencias que se han efectuado a instrumentos

internacionales, el derecho a la protección de datos personales, como derecho fundamental de tercera generación, se encuentra íntimamente ligado a dos factores: el desarrollo tecnológico y el comercio.

De esta forma, estas comisiones unidas estiman que está plenamente justificada la propuesta que se analiza a efecto de que se dote al Congreso de la Unión de facultades en materia de protección de datos en posesión de los particulares, considerando la estrecha vinculación que el derecho a la protección de datos guarda con el comercio nacional e internacional, actividad que se ha visto ampliamente potenciada con la revolución tecnológica en la que vive inmersa la sociedad actual, también denominada sociedad de la información.

En ese sentido, se considera que la legislación que regule el derecho a la protección de datos en posesión de los particulares debe ser federal por la indisoluble conexión con las materias mercantil y de telecomunicaciones.

Cabe señalar, a manera de referente que en países con regímenes federales como el nuestro, distintos de aquellos que se ubican en el radio de la Unión Europea, en los que se cuenta con legislación en torno al derecho a la protección de datos personales, como lo es el caso de Argentina y Canadá, la legislación en materia de protección de datos personales es competencia federal.

Actuar en otro sentido, dejando abierta la posibilidad de que exista normatividad asimétrica al interior de la Federación, puede traer consigo implicaciones graves para el Estado Mexicano, fundamentalmente a nivel internacional, ya que entre las consecuencias que a corto plazo pueden producirse, estaría la imposibilidad de cumplir debidamente los compromisos internacionales adquiridos, al privarse a la Federación de la facultad de regir de manera uniforme las relaciones jurídicas que se generen derivado del tratamiento de datos personales por parte de los particulares.

Lo anterior, sin perjuicio de la potestad legislativa que las entidades federativas conserven, respecto de los datos personales en posesión de los entes públicos estatales y municipales, en respeto de la autonomía de la que se encuentran dotadas producto del Pacto Federal.

En ese orden de ideas, corresponderá a las Legislaturas de los Estados la elaboración de la legislación que regule la protección de los datos personales que los órganos de los gobiernos estatales y municipales en su interacción con los particulares obtengan para el ejercicio de las atribuciones que les fueron conferidas, labor que a juicio de estas Comisiones Unidas de Puntos Constitucionales y Estudios Legislativos, Segunda, tras la experiencia adquirida a través de las disposiciones establecidas en la materia en las leyes de transparencia, facilitará la tarea de las mismas.
Aunado a lo anterior, la competencia de las Legislaturas Estatales para regular la protección de datos personales en posesión de autoridades locales, se sustenta en que el Estado no tiene entre sus atribuciones, el recabar información sobre particulares con fines de comercio, es decir, la obtención de la misma se origina en razón de la interacción entre los órganos del Estado,

como autoridad, y los gobernados, lo que implica una diferencia sustantiva entre este tratamiento y aquél que dan a los datos personales los particulares.

Con la aprobación de una reforma como la que se propone, el legislador ordinario contará con los elementos para elaborar una ley de protección de datos personales de carácter federal, en la que las disposiciones correspondientes plasmen los principios, derechos, procedimientos, infracciones, la existencia de una autoridad independiente y de un régimen de transferencias internacionales de datos, conforme a los estándares internacionales en esta materia. Lo anterior, no sólo garantizará de manera homogénea el derecho a la protección de datos personales, en cualquier punto del territorio nacional, también otorgará certeza y seguridad jurídica a los particulares cuyos datos son objeto de transferencias internacionales.

No obstante que las comisiones dictaminadoras están de acuerdo con el contenido propuesto en la minuta en comento, con fundamento en el artículo 140 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos, resulta necesario plantear una adecuación de técnica legislativa.

La Cámara de Diputados plantea adicionar una fracción XXIX-Ñ al artículo 73 constitucional, sobre el particular es oportuno referir que ha sido aprobada por las Comisiones Unidas de Puntos Constitucionales, de Estudios Legislativos y de Estudios Legislativos, Segunda, la Minuta Proyecto de Decreto por el que se adiciona un párrafo noveno al artículo 4° y se reforma la fracción XXV y adiciona una fracción XXIX-Ñ al artículo 73 de la Constitución Política, en materia de cultura y derechos de autor; por lo que con el ánimo de no duplicar las fracciones, estas comisiones dictaminadoras cambian el artículo único del Decreto, ya que no altera el sentido ni la intención de la Colegisladora para quedar como sigue: “Se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos”.

Por las razones anteriormente expuestas, se considera procedente incorporar en el texto constitucional la propuesta de la minuta en estudio, por lo que las comisiones dictaminadoras sometemos a la consideración de esta Soberanía el siguiente **PROYECTO DE: DECRETO POR EL QUE SE ADICIONA LA FRACCION XXIX-O AL ARTICULO 73 DE LA CONSTITUCION POLITICA DE LOS ESTADOS UNIDOS MEXICANOS.**

Artículo Único.- Se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, para quedar como sigue:
Artículo 73. El Congreso tiene facultad:
I. a XXIX-N. ...
XXIX-O. Para legislar en materia de protección de datos personales en posesión de particulares.

Una vez aprobada la reforma al artículo 73, XXIX-O, se turnó a las legislaturas de los Estados, para efectos del segundo párrafo del artículo 135 constitucional y de lo cual se recibieron 19 votos aprobatorios correspondientes a las legislaturas de los estados de Aguascalientes, Chiapas, Chihuahua, Colima, Durango, Guanajuato,

Michoacán, Morelos, Nayarit, Nuevo León, Oaxaca, Puebla, Sinaloa, Tabasco, Tamaulipas, Tlaxcala, Veracruz, Yucatán y Zacatecas.

Motivo de lo anterior es que el jueves 30 de abril de 2009, se publicó en el Diario Oficial de la Federación el Decreto por el que se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos en los siguientes términos:

> Artículo Único.- Se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, para quedar como sigue:
> Artículo 73. El Congreso tiene facultad:
> I. a XXIX-N. ...
> XXIX-O. Para legislar en materia de protección de datos personales en posesión de particulares.
> XXX. ...

La siguiente reforma constitucional es la correspondiente a la adición de un segundo párrafo del artículo 16 constitucional. Dicha iniciativa se presentó en la cámara de senadores y fue presentada por los entonces Senadores Santiago Creel Miranda y Alejandro González Alcocer (PAN), Pablo Gómez Álvarez (PRD) y Pedro Joaquín Coldwell (PRI).

A continuación, se mencionarán algunos fragmentos del dictamen de la Comisión de Puntos Constitucionales, con proyecto de decreto que adiciona un párrafo segundo al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos. Aprobado en lo general y en lo particular con 340 votos en pro, 0 en contra y 2 abstenciones. Se turno a las Legislaturas de los Estados para los efectos de lo dispuesto en el artículo 135 constitucional. Gaceta Parlamentaria, 11 de diciembre de 2008. Discusión y votación, 11 de diciembre de 2008:

> **II. Valoración de la Minuta**
>
> La Minuta enviada por el Senado a esta Cámara, en su calidad de origen, tiene por objeto desarrollar en el máximo nivel de nuestra normatividad el derecho a la protección de los datos personales.
>
> Los argumentos que expone la Minuta en cuestión, plantean lo siguiente:
>
> "Con esta reforma quedarían establecidos derechos internacionalmente reconocidos con los que debe contar el gobernado para verdaderamente dotarlo de un poder de disposición sobre sus datos personales.
>
> "Por lo que resulta necesario reconocer un derecho a la protección de los datos personales y que este reconocimiento se incorpore en el texto constitucional, pues de esta manera se generaría una certeza indiscutible del derecho, le brindaría seguridad y estabilidad.
>
> "El derecho fundamental de la protección de datos personales comprende otros

derechos que corresponden a los gobernados, como acceder a los mismos y, en su caso, obtener su rectificación, cancelación u oposición en los términos que fijen las leyes.

"El derecho de oposición (…) tiene como objeto de facultar a los ciudadanos a manifestar su conformidad en torno al tratamiento de datos que han sido obtenidos de fuentes accesibles al público para fines de publicidad.

"Otra de las razones que justifica la existencia del derecho de oposición es (que) se emplea como una herramienta para combatir determinaciones basadas únicamente en un tratamiento automatizado de datos destinado a evaluar ciertos aspectos relativos a la personalidad, como el rendimiento laboral, fiabilidad, conducta, entre otros.

"Estas comisiones unidas la consideran adecuada, ya que la protección de datos personales puede estar sujeta a excepciones bajo ciertos supuestos y condiciones, esto es sólo en los casos en los que por su trascendencia este derecho se encuentre en contraposición con otros derechos y amerite una ponderación de la autoridad teniendo presente el bien común, como es el caso de la seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de tercero. Puesto que la categoría de un derecho fundamental no puede ser un derecho superior a cualesquier otro o bien a intereses sociales o públicos.

"Conviene recordar que al adquirir el derecho a la protección de datos personales el carácter de un derecho fundamental, resulta indispensable que las excepciones a la aplicación de los principios que rigen la materia sean establecidas al mismo nivel jerárquico, es decir, en la Ley Fundamental, a efecto de que en virtud del principio de supremacía constitucional, previsto en el artículo 133 de la Carta Magna, se asegure desde el máximo nivel normativo cuáles son los límites a los que se pueden someter los citados principios, así como los parámetros en función de los que deberá desarrollarse cualquier instrumento normativo. En el caso que nos ocupa queda claro además que existe una reserva de ley en la materia, es decir, que el desarrollo de los supuestos de excepción establecidos en la Constitución deberán ser desarrollados únicamente en instrumentos de rango legislativo.

"… ante este creciente avance tecnológico ha sido necesario dar respuesta a los nuevos retos que debe enfrentar la libertad de las personas como consecuencia de los cambios que la tecnología ha ido introduciendo. México debe así adecuar su marco constitucional para otorgar a toda persona una protección adecuada contra el posible mal uso de su información." […]

Un primer paso, con alcances limitados en esta materia, se dio con la entrada en vigor de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, en la cual por primera vez en México se reconoció la existencia de este derecho, en el contexto del acceso a la información pública.
Derivado del reconocimiento legal, que para efectos de acceso a la información se planteó, dio inicio un interesante desarrollo del derecho a la protección de datos en el ámbito administrativo, por primera vez en la historia de este país los particulares gozaban del derecho a acceder y rectificar los datos personales

que obraran en los sistemas de datos personales del Estado.

El segundo y fundamental paso, al que ya hicimos alusión, se presentó con la aprobación de la reforma al artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, en el que también por primera ocasión un texto constitucional hace referencia expresa al derecho a la protección de datos, en este caso, como un límite al derecho de acceso a la información.

Por ello, la propuesta que se presenta ante esta Cámara revisora, tiene como propósito consolidar el derecho a la protección de datos en nuestro país, extendiendo su ámbito de aplicación a todos los niveles y sectores, apuntalando, por una parte, la estructura edificada a través del artículo 6o. fracción II de la Constitución Federal y de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, para los sistemas de datos personales en posesión de los entes públicos federales y, por la otra, reconociendo la existencia del mismo respecto de los datos personales en poder de particulares.

Este nuevo derecho, consiste en la protección a la persona, en relación con la utilización que se dé a su información personal, tanto por entes públicos como privados.

En términos de lo anterior, la estructura propuesta serviría de punto de partida para cualquier regulación que se emita en torno al derecho a la protección de datos, tanto en el ámbito público como en el privado, considerando que hasta ahora no se cuenta con una disposición a nivel constitucional en la que se establezcan el contenido y los alcances de este derecho, en cuanto a los principios, derechos y excepciones por los que se debe regir todo tratamiento de datos personales. […]

En ese sentido, la iniciativa que se dictamina permitiría concluir el trabajo iniciado con la reciente reforma al artículo 6o. de la CPEUM, ya que se reconoce el derecho de acceso a la información pública y por su parte el artículo 16 establecerá el derecho a la protección de datos personales, que, aunque mencionado en la fracción II del 6o. se estaría dotando finalmente de contenido a este derecho fundamental. […]

Con esta reforma se está reconociendo al gobernado el derecho a disponer de manera libre, informada y específica sobre el tratamiento de los datos personales que le conciernan, sobre la base del consentimiento el cual activa diversas modalidades de tratamiento, así como cursos de acción. En ese sentido, existen diversas formas en las que el consentimiento puede ser otorgado, situación cuya determinación dependerá de distintos factores como la naturaleza de los datos, la fuente de la que se obtuvieron, la finalidad del tratamiento, entre otros. Así, cabe distinguir entre consentimiento presunto, tácito, expreso y expreso y por escrito (sin que el consentimiento por escrito tenga que plasmarse en papel). En cualquiera de los casos señalados, la cuestión se centra en la prueba de la obtención del consentimiento. Es decir, tanto en el consentimiento tácito, principalmente, como en el expreso que no sea escrito, hay que implementar procedimientos estandarizados para la obtención de dicho consentimiento para que luego se pueda probar que se

cuenta con el mismo. Dicha prueba recae en quien solicita el consentimiento para el tratamiento de datos de carácter personal, es decir, el responsable del archivo. Por tanto, deberá hacerse uso de vías que permitan acreditar que se solicitó del interesado una manifestación en contra para oponerse al tratamiento de sus datos, de manera que su omisión pueda ser entendida como consentimiento al tratamiento, dando un plazo prudencial para que el interesado o titular del dato pueda conocer que su omisión implica la aceptación del tratamiento.

A manera de ejemplo basta con citar el caso del tratamiento de datos personales con fines de publicidad o marketing, en los que habiéndose recabado el dato de una fuente de acceso público, se entiende consentido el tratamiento con dichos fines, hasta en tanto el titular del mismo no manifieste su oposición. Al observar lo anterior, se logra un equilibrio que favorece el crecimiento económico que permite un flujo dinámico de información y por ende, que facilita las transacciones comerciales en diversos segmentos de mercado.

El principio del consentimiento se vería complementado por los principios de información, calidad, seguridad y confidencialidad, a través de los cuales es posible al titular de los datos personales: […]

Por lo anteriormente expuesto y motivado de acuerdo con la Constitución, La Ley Orgánica y el Reglamento para el Gobierno Interior del Congreso General, todos los ordenamientos de los Estados Unidos Mexicanos, esta Comisión somete a consideración del Pleno de la Cámara de Diputados, el siguiente:

Proyecto de Decreto que adiciona un párrafo segundo al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos

Artículo Único: Se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, para quedar como sigue:

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.

No podrá librarse orden de aprehensión sino por la autoridad judicial y sin que preceda denuncia o querella de un hecho que la ley señale como delito, sancionado con pena privativa de libertad y obren datos que establezcan que se ha cometido ese hecho y que exista la probabilidad de que el indiciado lo cometió o participó en su comisión. (...)

Una vez aprobada la reforma al artículo 73, XXIX-O, se turnó a las legislaturas de los Estados, para efectos del segundo párrafo del artículo 135 constitucional y de lo cual se recibieron 18 votos aprobatorios correspondientes a las legislaturas de Aguascalientes, Baja California, Coahuila, Colima, Chiapas, Chihuahua, Durango, Guanajuato, Michoacán, Morelos, Nuevo León, Oaxaca, Sinaloa, Tabasco, Tamaulipas, Tlaxcala, Yucatán y Zacatecas, con los que se aprueba la minuta con proyecto de decreto que adiciona un párrafo segundo al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos.

Motivo de lo anterior es que el lunes 01 de junio de 2009, se publicó en el Diario Oficial de la Federación el 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. en los siguientes términos:

> Artículo Único.- Se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, para quedar como sigue:
>
> 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.
>
> No podrá librarse orden de aprehensión sino por la autoridad judicial y sin que proceda denuncia o querella de un hecho que la ley señale como delito, sancionado con pena privativa de libertad y obren datos que establezcan que se ha cometido ese hecho y que exista la probabilidad de que el indiciado lo cometió o participó en su comisión. (...)

Con fecha 4 de noviembre de 2008, el Diputado Federal Luis Gustavo Parra Noriega, integrante del Grupo Parlamentario del Partido Acción Nacional, presentó iniciativa con proyecto de Decreto, por la que se expide la Ley de Protección de Datos Personales en Posesión de los Particulares (en adelante LFPDPPP).

En el dictamen de proyecto de la Cámara de Diputados se relacionan diferentes aspectos como:

1) Antecedentes en la protección de datos personales a nivel internacional
    a. Países donde se ha regulado
    b. Tratados internacionales como el Convenio 108 de Europa
2) Sujetos que se exceptúan de la aplicación de la que será la LFPDPPP
3) Principios y alcances de cada principio de protección de Datos personales

a. Licitud
b. Consentimiento
c. Calidad
d. Finalidad
e. Proporcionalidad
f. Responsabilidad
g. Información
h. Lealtad

4) Manejo de Datos Personales Sensibles
5) Derecho al Olvido
6) Procedimiento ante el responsable y protección de derechos
7) Autoridades reguladoras
8) Medidas de seguridad
9) Infracciones y sanciones

La Ley de Protección de Datos Personales en Posesión de los Particulares se publicó en el Diario Oficial de la Federación el 05 de julio de 2010 y su Reglamento el 21 de diciembre de 2011.

Para finalizar este apartado es importante mencionar que si bien la LFPDPPP regula de manera general la protección de datos personales; existen también otras disposiciones que regulan el mismo tópico de manera más específica como la Ley para Regular las Sociedades de Información Crediticia; Ley General de Salud, Ley General de los Derechos de Niñas, Niños y Adolescentes; disposiciones que serán analizadas en el rubro respectivo de esta Tesis.

1.3 Desarrollo de la Transparencia y el Acceso a la Información Pública Gubernamental

Haydeé Pérez y Renata Terrazas comentan que "el acceso a la información, la transparencia y la rendición de cuentas son elementos indispensables para avanzar en la construcción de una democracia sustantiva. Asimismo, estos accesos son esenciales para lograr un gobierno responsable y responsivo a las necesidades de la ciudadanía y de una sociedad interesada en participar activamente en los asuntos públicos que afectan su calidad de vida."[80]

Se dice que el término de transparencia es curiosamente uno de los términos más opacos de todos; *arcana imperii*, razones de Estado, y otra serie de nombres por las que cierta información no debe hacerse pública desde tiempos inmemoriales, han hecho que la transparencia sea un problema de matices públicos entre los que detentan el poder y una sociedad cada vez más hambrienta de concomimiento y sed de saber.

[80] Pérez Haydeé y Terrazas Renata, *Acceso a la Información y transparencia en México*, Razones FUNDAR, México, s/d, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.fundar.org.mx/mexico/pdf/transparencyacceso.pdf* p. 1.

La pregunta es ¿saber qué?, simplemente saber lo que sea (dicho coloquialmente) que pueda ser relevante para la sociedad de todos los temas posibles: contratos, servicios, trámites, procedimientos, presupuesto y un largo etc., etc., que si bien durante un largo tiempo se dijo que la opacidad era ocultar información; hoy parece que la moneda ha cambiado de lado; es decir, que si se quiere ocultar información ahora hay que ponerla a la vista de todos. En este sentido, ante la apertura máxima de la información, podría decirse que hoy estamos en presencia de la opacidad positiva.

No obstante, hay que recordar que la información "es un instrumento, un instrumento que nos da recursos para la transparencia, un instrumento a partir del cual tenemos insumos para entender mejor la realidad, para reaccionar de distintas maneras ante ella, pero solamente y esto es muy importante, es un instrumento."[81]

¿Qué conviene dar a conocer? ¿Qué se quiere dar a conocer? ¿Por qué se quiere dar a conocer cierta información? ¿Qué información no debe darse a conocer incluso bajo riesgo de perder la vida?

Son estas y un sinfín de preguntas más las que han ido moldeando la transparencia, el acceso a la información y de manera adicional, el cuidado de la información en archivos (documentos) por lo que la humanidad a luchado y a muerto por esconder y por dar a conocer la información, cualquiera que esta sea, de todo tipo, y ante diferentes tipos de actores; es por ello que en este apartado daremos un breve recorrido histórico normativo sobre la transparencia y acceso a la información.

1.3.1. En el Mundo

Cristóbal Cruz Revueltas inicia su disertación sobre transparencia, política y valores con el desafío de Giges de la siguiente manera:

> Cuenta el filósofo griego Platón (427-347 a. C.)- es de notar que lo hace en voz de hermano Glaucón- que un buen día, tras un terremoto, se abrió una enorme grieta en el campo en el que un pastor de nombre Giges solía llevar su ganado. Al ver la abertura, Giges, intrigado, se adentró en ella y, para su asombro, en su interior encontró, entre otras maravillas, un anillo de oro. Pronto descubrió que al ponerse la sortija y con tan solo girar su engaste al interior, el portador adquiría la virtud mágica de hacerse invisible y de nuevo visible al girarlo hacia el exterior. Una vez seguro del velo protector que le ofrecía el anillo, quien hasta entonces no había sido sino un tranquilo pastor ocupado de su rebaño, pronto se las ingenió para acceder al palacio del rey, corromper a la reina y apoderarse del trono. Este relato hace patente que ya, desde la Grecia clásica, es bien conocido que el ejercicio oculto del poder,

[81] Trejo Delarbre, Raúl *et. al. Democracia, acceso a la información y tecnología*, en "Transparencia y acceso a la información, las tendencias en el mundo", [en línea] México, IIJ-UNAM, 2005, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://archivos.juridicas.unam.mx/www/bjv/libros/6/2503/3.pdf* p.30.

> fuera del espacio público visible, se presta fácilmente a la ruptura de los vínculos sociales de la confianza y, por lo mismo, a la corrupción y a la arbitrariedad.[82]

Diversos autores reconocen en Platón como el primer defensor de la escuela filosófica de la "sociedad cerrada" es decir; de un régimen "antidemocrático, organicista y totalitario que ahoga las libertades individuales con los argumentos de que la verdad solo está en el Estado, de que éste debe ser gobernado sólo por una élite de sabios y de que la justicia consiste en que cada uno ocupe el lugar que le corresponde en una jerarquía social de escalones inamovibles."[83]

El mismo Rodríguez Zepeda en su obra "Estado y Transparencia" aborda magistralmente el concepto del *Arcana Imperii*, siguiendo las ideas platónicas como se muestra a continuación:

> El conocimiento de las verdades de la política queda así reservado a quienes, partícipes de la aristocracia del intelecto, pueden trascender los prejuicios e ignorancia del populacho. Este es el sentido de la justicia que está en el origen de los *arcana imperii*, es decir, de los secretos del poder que establecen un adentro y un afuera en el poder político, y, por lo tanto, jerarquizan a las personas en relación con la práctica política y con la calidad de los conocimientos y argumentos que pueden tener a su disposición.
> Por ello, no es en lo absoluto banal la famosa frase que reza "saber es poder". Los *arcana imperii* son verdades y conocimientos, informaciones y evaluaciones, argumentos y discursos, exclusivos de los hombres del poder. Y estos elementos del saber no son accesorios o laterales para el ejercicio del poder y del dominio, son más bien la condición que los hace posibles.
> Aristóteles (384-322 a.c.) llamó *sophismata* a estas claves, exclusivas y excluyentes, que hacen posible el ejercicio del poder político. En su libro *La política* las asoció con los "artificios" de las constituciones democráticas para privilegiar el peso político de los pobres para degradar la aristocracia y promover la democracia (1297ª) y que las "sofisterías constitucionales" destinadas a engañar al pueblo y que impiden garantizar la seguridad de las propias constituciones (1308ª). Se trata, en todo caso, de ofertas aparentes de derechos que ocultan una intención desconocida para quien las recibe. Son, en suma, secretos que permiten el ejercicio del poder sobre la base del ocultamiento y la simulación.
>
> Las *sophismata* de Aristóteles son piezas de conocimiento, del saber cómo forma de poder, que hacen posible que se gobierne a los súbditos según los

[82] Cruz Revueltas, Juan Cristóbal, *Moral y transparencia. Fundamento e implicaciones morales de la transparencia*, [en línea] Cuadernos de Transparencia, México, INAI, 2015, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/Cuadernillo%2015%20B.pdf* p. 10.
[83] Rodríguez Zepeda, Jesús, *Sensibilización para la transparencia y rendición de cuentas. Manual del Participante* [en línea] México, INAI. 2015, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.sep.gob.mx/work/models/sep1/Resource/18094/4/images/m-sensibilizacion.pdf* p. 14.

> intereses particulares de los gobernantes y que se marque una distancia insalvable entre quienes son gobernados y quienes gobiernan.
>
> Fue el gran historiador latino Tácito (50-120), el primero que denominó *arcana imperii* a estas piezas del saber, a estos misterios de la política. *Arcana* (Proviene de una raíz indo-europea: *arek*) significa secreto, algo que se retiene o que se guarda, Pero *arcana imperii* no se reducen a la condición de información llana sobre las cuestiones públicas, sino a la información selecta, privilegiada, que define como sujeto de poder a quien la posee y administra. La posesión o el acceso a los *arcana imperii* inviste de poder a sus sujetos, pies no es sólo una relación cognoscitiva (saber más que otros), sino una relación política (dominar o gobernar a otros en razón de ese saber).
>
> Los *arcana imperii* se asemejan, en este sentido, a los *arcana ecclesiae*, es decir, a las razones y verdades profundas que invisten de sacralidad a los ministros religiosos que los detentan.
> Estos misterios de la política fueron llamados *libertatis umbra* por Plinio (23-79) en su obra *Naturalis Historia*, y *blandimenta imperii* por el neoplatónico Justino (105-165). Son el tipo de conocimientos o informaciones que, en la época moderna, fueron denominados, sencillamente, secretos de Estado. Y son, en buena medida, el origen de la llamada "razón de Estado". […]
>
> En efecto, la existencia misma de los *arcana imperii* nos habla, por una parte, de un poder cuyos intereses y motivaciones (y a veces hasta sus reales poseedores) permanecen ocultos a los gobernados, y, por otra, de ese mismo poder que de manera sistemática sustrae información y sus razones del escrutinio de los ciudadanos como forma de conservar el dominio en la sociedad.[84]

En la Edad Media el pensamiento político estuvo dominado por la *Arcana* en sus dos vertientes formadas en la etapa de la Roma imperial, la *imperii* y la *ecclesiae*, siendo ambos "misterios trascendentes, dogmas de fe y verdades indiscutibles".[85]

La Edad Media es una época convulsa en todos sentidos, políticos, económicos, culturales. Los otrora denominados pueblos bárbaros, se asentaron en los antiguos dominios romanos y se mezclaron las culturas viejas con las nuevas; el poder de la Iglesia se afianzó y la nueva amenaza, el Islam sería crucial para la reconfiguración del mundo conocido.

Con el término de la edad oscura, las ciudades estado van tomando forma de la nueva configuración del Estado y con ello pensadores como Maquiavelo y Hobbes

[84] Rodríguez Zepeda, Jesús, *Estado y Transparencia: Un paseo por la filosofía política*, [en línea] Cuadernos de Transparencia, México, Número 4, INAI. 2015, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/Cuadernillo%2004%20B.pdf* pp. 13-14.
[85] *Ibidem*, p. 15.

irrumpen en la escena con sus singulares pensamientos que apoyarían en la formación del concepto razón de Estado, prácticamente al mismo tiempo que avanzaba el concepto de estado absolutista.

La razón de Estado, no es sólo una forma de reservar para los políticos una serie de argumentos propios, sino que es, fundamentalmente, la convección de la supremacía de las razones del poder sobre cualesquiera otras razones o intereses. Por ello, las razones del Estado pueden chocar con las razones legales o el sentido de la ley. Si existe algo así como "interés superior del Estado" o el "bien del Estado" los gobernantes deberían perseguirlo siempre, incluso pasando por sobre cualquier norma legal o moral que pudiera levantarse como obstáculo.[86]

Sobre este concepto, cuenta la Historia que cuando Carlos III de Espala expulsó de sus dominios a los jesuitas, se le preguntó el motivo de tal medida a lo cual expresó lo siguiente: "Por razones que guardo en mi real pecho". "Dicha frase resume la posición constante adoptada por los gobernantes a lo largo de muchos siglos en la historia de la humanidad, misma que en la actualidad se considera inadmisible e inclusive absurda, en razón del derecho fundamental denominado como derecho de acceso a la información pública."[87]

Aquí vale la pena abrir un pequeño paréntesis para mencionar a Martínez Becerril, el cual comenta que "contrario a lo que uno pensaría respecto de un derecho relativamente novedoso y sofisticado, éste no fue concebido primigeniamente en un país europeo o siquiera occidental, sino que surge materialmente como una inspiración de prácticas e instituciones burocráticas de la China Imperial".[88]

Al respecto, Martínez Legorreta, citado por Martínez Becerril indica que "entre las prácticas e instituciones burocráticas chinas, destaca el denominado Ministerio de Censura, el cual "estaba a cargo de la red de vigilancia, pero había también verificaciones internas a través de toda jerarquía administrativa. Había investigaciones casi a diario sobre la competencia de los funcionarios oficiales, así como informes cada tres años sobre los méritos y fallas en toda la jerarquía".[89]

Con el advenimiento del liberalismo se aprecia un nuevo giro en el desarrollo de la transparencia y la privacidad, se comienza a dar razones que la parte pública modifica a la privada y viceversa, a mayor peso de lo público se presenta un menor peso de lo privado.

---

[86] *Ibidem*, p. 18.
[87] Martínez Becerril, Rigoberto, *El derecho de Acceso a la Información en México, su ejercicio y medios de impugnación*, [en línea] México, INFOEM, 2009, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.infoem.org.mx/sipoem/ipo_capacitacionComunicacion/pdf/pet_tesis_001_2008.pdf* p. 17.
[88] *Ídem*.
[89] Martínez Legorreta, Omar, *El servicio civil en la China Imperial*, en Martínez Becerril, Rigoberto, *op. cit*, p. 19.

Rodríguez Zepeda menciona lo siguiente:

> Para los efectos del tema de la verdad, de las doctrinas y de la información, el liberalismo introduce la novedad de que no existen verdades de Estado, ni, por ello, secretos que deban ser preservados de la mirada e interés de los ciudadanos comunes, ni tampoco, en todo caso, sujetos privilegiados en cuanto al manejo de la información pública.
>
> El liberalismo, en su vertiente más ilustrada, es decir, como teoría del gobierno mandatario y de los derechos inviolables de la persona, es enemigo de los *arcana imperii*. Por ello, no es de extrañar que las regulaciones legales antiguas y los más poderosos mecanismos de control social sobre la información pública se hayan dado en naciones con influencia de este tipo de tradición política.[90]

De ahí que para 1776, Anders Chydenius, quien era un sacerdote sueco, haya tomado las prácticas chinas argumentando que China era un país modelo en lo tocante a la libertad de prensa y por ello haya impulsado la que se considera la primera ley de acceso a la información llamada Ley para la Libertad de Prensa y del Derecho de Acceso a las Actas Públicas (*Freedom-of-press and the right-of-access to public records Act* o en sueco *Tryckfrihetsförordningen*).

Al respecto John Ackerman e Irma Sandoval documentan que esta ley:

> Era un producto del movimiento político liberal, comandado por Gustavo III, el mismo que configuró una nueva Constitución. En ella se reforzaba el papel del *Riksdag* (Parlamento), la discusión de los asuntos públicos -como la guerra- debía ser atraída al máximo órgano de representación y, como corolario de todo, quedaba reducido para siempre el vetusto "comité secreto de los tres primeros estados".
>
> Años después de la Constitución Chydenius y los suyos dieron un paso más allá: inspirado e impresionado por la experiencia China, quiso instaurar algo así como el Buró de Censura Imperial, una institución de la dinastía *Ch'ing* (sic) que se encargaba de vigilar cuidadosamente al gobierno y a sus funcionarios, de exhibir sus incompetencias, ineficiencias y prácticas de corrupción.[91]

Es importante destacar que esta ley sueca de 1776, fue publicada 10 años antes de la independencia de los Estados Unidos y 13 años antes de la Revolución francesa, lo que denota que las prácticas orientales chinas fueron bien tomadas por Suecia quien la transformó a su realidad y con ello se convirtió en el primer país de occidental al convertirse en la punta de lanza para los años por venir y ejemplo para

[90] Martínez Becerril, Rigoberto, *op. cit.* p. 28.
[91] Ackerman M., John y Sandoval, Irma E., *Leyes de acceso a la información en el mundo*, [en línea] México, Cuadernos de Transparencia, Número 7, INAI, 2015, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/Cuadernillo%2007.pdf* p. 5.

las naciones de pensamiento occidental sobre cómo ir abriendo la coraza e ir publicitando el actuar de los entes públicos.

Ackerman menciona que las leyes de acceso a la información contemporáneas surgen de las viejas batallas por las libertades de expresión, de prensa y por el derecho a participar en la toma de las decisiones públicas.

> Con el surgimiento del "Estado Administrativo" el vínculo entre la libertad de expresión, la participación ciudadana en asuntos públicos y la libertad de acceso a la información gubernamental se vuelve aún más importante. Sólo si los ciudadanos cuentan con acceso a la información en resguardo del gobierno, es que podemos hablar de ciudadanos democráticos, En la era del "Estado Administrativo", las libertades de expresión y de participación quedan sin mayor significado si éstas carecen de la información concerniente a las mecánicas internas del gobierno.[92]

Desde el punto de vista contemporáneo, la Declaración Universal de los Derechos Humanos de 1948 constituye el que ha sido considerado como el primer documento de carácter global que reconoce el derecho a la información.

El artículo 19 dispone lo siguiente:

> Artículo 19
> Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión.[93]

Por su parte el Pacto Internacional de Derechos Civiles y Políticos adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General de la ONU en su resolución 2200 A (XXI), de 16 de diciembre de 1966 dispone:

> Artículo 19
> 1. Nadie podrá ser molestado a causa de sus opiniones.
> 2. Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.
> 3. El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para:
> a) Asegurar el respeto a los derechos o a la reputación de los demás;
> b) La protección de la seguridad nacional, el orden público o la salud o la

[92] *Ibidem*, p. 15.
[93] Organización de las Naciones Unidas, *Declaración Universal de Derechos Humanos*, [en línea] s/d, [fecha de consulta: 15 de junio de 2021] Disponible en: *https://www.ohchr.org/en/udhr/documents/udhr_translations/spn.pdf* p. 6.

moral públicas.[94]

En la encíclica papal "*Pacem in Terris*", emitida el 11 de abril de 1963, se hizo la afirmación de los elementos constitutivos de este nuevo derecho: "el derecho del ser humano a una información objetiva". En este proceso evolutivo de la libertad de expresión, merece citarse también la proclamación, por parte del Vaticano, del derecho que tienen todos a una información objetiva. En 1964 el Papa Pablo VI, con motivo de un seminario de las Naciones Unidas sobre la libertad de información, dijo lo siguiente:

"El derecho a la información es un derecho universal, inviolable e inalterable del hombre moderno, puesto que se funda en la naturaleza del hombre. Se trata de un derecho activo y pasivo: por una parte, la búsqueda de la información; y por la otra, la posibilidad de todos a recibirla".[95]

El mandato de la UNESCO, tal como se establece en su Constitución de 1945, apela expresamente a la Organización para que "promueva la libre circulación de ideas por medio de la palabra e imagen". La libertad de información también es fundamental en el marco de la Cumbre Mundial de la Sociedad de la Información, la cual reafirma el acceso universal a la información como piedra angular de sociedades del conocimiento inclusivas. Además, la importancia del Acceso a la información también se destaca en la Declaración de Brisbane sobre la Libertad de Información: El derecho a saber de 2010, la Declaración de Maputo sobre el Fomento de la Libertad de expresión, Acceso a la información y Emancipación de las personas de 2008 y la Declaración de Dakar sobre los Medios de comunicación y buen gobierno de 2005.[96]

Ahora bien, reconociendo la importancia del acceso a la información, la 74a Asamblea General de la ONU proclamó el 28 de septiembre como el Día Internacional para el Acceso Universal a la Información (IDUAI) a nivel de la ONU en octubre de 2019. El día había sido proclamado por la Conferencia General de la UNESCO en 2015, a continuación, la adopción de la Resolución 38 C / 57 que declara el 28 de septiembre de cada año como Día Internacional del Acceso Universal a la Información (IDUAI). [97]

---

[94] Organización de las Naciones Unidas, *Pacto Internacional de Derechos Civiles y Políticos*, [en línea] s/d/, [fecha de consulta: 15 de junio de 2021] Disponible en: *https://www.ohchr.org/sp/professionalinterest/pages/ccpr.aspx*

[95] Fuenmayor E. Alejandro, *El derecho de acceso de los Ciudadanos a la Información Pública*, [en línea] Costa Rica, UNESCO, 2004, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.iidh.ed.cr/derecho-informacion/media/1077/acceso_informacion_desarrollos_otros_unesco_propuesta_ley_modelo.pdf* p. 15.

[96] UNESCO, *Leyes de acceso a la información*, [en línea] UNESCO, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://es.unesco.org/themes/leyes-acceso-informacion*

[97] s/a, *International Day for Universal Access to Information*, UNESCO, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://en.unesco.org/commemorations/accesstoinformationday*

Proclamación del Día Internacional del Acceso Universal a la Información

La Conferencia General,

Habiendo examinado el documento 38 C/70,

Recordando que el derecho a la información es parte integrante del derecho a la libertad de expresión, reconocido en la resolución 59 de la Asamblea General de las Naciones Unidas, aprobada en 1946, y definido en el Artículo 19 de la Declaración Universal de Derechos Humanos y el Artículo 19 del Pacto Internacional de Derechos Civiles y Políticos,

Recordando también que la libertad de información ocupa un lugar central en el marco de la Cumbre Mundial sobre la Sociedad de la Información (CMSI), en la que se reafirmó que la libertad de expresión y el acceso universal a la información son piedras angulares para construir unas sociedades del conocimiento integradoras,

Teniendo presentes los esfuerzos realizados por la UNESCO para poner de relieve la pertinencia y la importancia del derecho a la información por medio de la Declaración de Brisbane – Libertad de información: el derecho a saber (2010), la Declaración de Maputo: Promover la libertad de expresión, el acceso a la información y la emancipación de las personas (2008), y la Declaración de Dakar – Medios de comunicación y buen gobierno, entre otras,

Tomando nota de la Declaración de la Plataforma Africana sobre el Acceso a la Información, aprobada en la Conferencia Panafricana sobre el Acceso a la Información en África organizada por la Campaña Windhoek+20 para el acceso a la información en África, en colaboración con la UNESCO, la Comisión de la Unión Africana y la Relatora Especial sobre Libertad de Expresión y Acceso a la Información en África, que tuvo lugar en Ciudad del Cabo (Sudáfrica) del 17 al 19 de septiembre de 2011,

Teniendo en cuenta el hecho de que el acceso a la información es una de las prioridades principales de las actividades de la UNESCO,

Teniendo en cuenta también que diversas organizaciones de la sociedad civil y organismos gubernamentales de distintos lugares del mundo han adoptado y celebran actualmente el 28 de septiembre como “Día internacional del derecho a saber”,

Tomando nota también de los principios establecidos en la Declaración de la Plataforma Africana sobre el Acceso a la Información y reconociendo que estos principios pueden cumplir una función crucial para el desarrollo, la democracia, la igualdad y la prestación de los servicios públicos,

1. Decide proclamar el 28 de septiembre de cada año Día Internacional del Acceso Universal a la Información;

2. Invita a todos los Estados Miembros, a los organismos del sistema de las Naciones Unidas y a otras organizaciones internacionales y regionales, así como a la sociedad civil, incluidas las organizaciones no gubernamentales y los particulares, a celebrar este día del modo que cada uno considere más apropiado, y sin repercusiones financieras para el presupuesto ordinario de la UNESCO;

3. Pide a la Directora General que señale esta resolución a la atención del Secretario General de las Naciones Unidas, de modo que la Asamblea General también pueda refrendar el Día Internacional del Acceso Universal a la Información.

Resolución aprobada, previo informe de la Comisión CI, en la 16ª sesión plenaria, el 17 de noviembre de 2015.[98]

La UNESCO y sus programas intergubernamentales, el Programa Internacional para el Desarrollo de la Comunicación y el Programa Información para Todos, proporcionan una plataforma y un marco para que todas las partes interesadas participen en los debates internacionales sobre políticas y directrices en el ámbito del acceso a la información.[99]

Por su parte, en lo que hace al Sistema Interamericano, en 1948 los Estados americanos adoptaron la Declaración Americana de los Derechos y Deberes del Hombre, cuyo artículo IV establece que: Toda persona tiene derecho a la libertad de investigación, opinión, expresión y difusión del pensamiento por cualquier medio.

En 1969 se suscribió la Convención Americana sobre Derechos Humanos. En el numeral 1 del artículo 13 del mencionado instrumento claramente se expresa que: Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.[100]

La Carta Democrática Interamericana (2001) dispone: Artículo 3. “Los Estados Parte convienen en considerar la aplicabilidad de medidas, dentro de sus propios sistemas institucionales, destinadas a crear, mantener y fortalecer normas de conducta para el correcto, honorable y adecuado cumplimiento de las funciones públicas y Mecanismos para hacer efectivo el cumplimiento de dichas normas de conducta.”

A su vez, la Declaración de la Cumbre de las Américas de Nuevo León (2004) versa:

---

[98] UNESCO, *Actas de la Conferencia General*, París, UNESCO, 38ª reunión, Vol 1. Resoluciones, 2016, *https://unesdoc.unesco.org/ark:/48223/pf0000243325_spa* pp. 57-58.
[99] UNESCO, *Leyes de acceso a la información, op. cit.*
[100] Organización de Estados Americanos, *Estudio Especial sobre el derecho de acceso a la información*, [en línea] EUA, OEA, Relatoría Especial para la Libertad de Expresión, 2007, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *http://www.cidh.oas.org/relatoria/section/Estudio%20Especial%20sobre%20el%20derecho%20de%20Acceso%20a%20la%20Informacion.pdf* p. 14.

"El acceso a la información en poder del Estado, con el debido respeto a las normas constitucionales y legales, incluidas las de privacidad y confidencialidad, es condición indispensable para la participación ciudadana y promueve el respeto efectivo de los derechos humanos."[101]

Por último, tomando como base el índice del Derecho a la Información de *Global RTI Rating*, elaborado por el *Access Info Europe* y el Centro para la Ley y la Democracia colocaré un cuadro con los países y años de adopción de su ley de transparencia y acceso a la información.[102]

Países	Año Ley	Países	Año Ley
Suecia	1766	Finlandia	1951
Estados Unidos	1966	Dinamarca	1970
Noruega	1970	Francia	1978
Países Bajos	1978	Australia	1982
Nueva Zelanda	1982	Canadá	1983
Colombia	1985	Grecia	1986
Austria	1987	Italia	1990
Hungría	1992	Ucrania	1992
Portugal	1993	Bélgica	1994
Belice	1994	Islandia	1996
Corea del Sur	1996	Lituania	1996
Tailandia	1997	Uzbekistán	1997
Israel	1988	Letonia	1998
Japón	1999	Albania	1999
República Checa	1999	Georgia	1999
Liechtenstein	1999	Trinidad y Tobago	1999
Reino Unido	2000	Bosnia y Herzegovina	2000
Bulgaria	2000	Estonia	2000
Moldavia	2000	Eslovaquia	2000
Sudáfrica	2000	Polonia	2001
Rumania	2001	Angola	2002
Jamaica	2002	México	2002
Panamá	2002	Pakistán	2002
Tayikistán	2002	Zimbabue	2002
Armenia	2003	Croacia	2003
Irlanda	2003	Perú	2003

[101] Organización de Estados Americanos, *Leyes de Acceso a la Información*, OEA*,* [fecha de consulta: 3 de diciembre de 2022] Disponible en: *http://www.oas.org/es/sap/dgpe/acceso/mandatos.asp*

[102] Revista Expansión (no se menciona el nombre del autor), *Índice del Derecho a la Información, Ranking del Derecho a la Información 2019*, [en línea] México, Revista Expansión, 2019, [fecha de consulta: 3 de diciembre de 2022] Disponible en:*https://datosmacro.expansion.com/estado/indice-derecho-informacion?anio=2019*

Países	Año Ley	Países	Año Ley
Serbia	2003	Eslovenia	2003
Turquía	2003	San Vicente y las Granadinas	2003
Antigua y Barbuda	2004	Argentina	2004
Suiza	2004	República Dominicana	2004
Ecuador	2004	Alemania	2005
Azerbaiyán	2005	Bolivia	2005
India	2005	Montenegro	2005
Taiwán	2005	Uganda	2005
Honduras	2006	Macedonia del Norte	2006
China	2007	Jordania	2007
Kirguistán	2007	Nicaragua	2007
Nepal	2007	Chile	2008
Etiopía	2008	Guatemala	2008
Indonesia	2008	Malta	2008
Uruguay	2008	Bangladés	2009
Irán	2009	Rusia	2009
Guinea	2019	Liberia	2010
Brasil	2011	Mongolia	2011
Níger	2011	Nigeria	2011
El Salvador	2011	Túnez	2011
Yemen	2012	España	2013
Costa de Marfil	2013	Guyana	2013
Ruanda	2013	Sierra Leona	2013
Sudán del Sur	2013	Afganistán	2014
Maldivas	2014	Mozambique	2014
Palaos	2014	Paraguay	2014
Burkina Faso	2015	Benín	2015
Kazajistán	2015	Kenia	2016
Sri Lanka	2016	Filipinas	2016
Togo	2016	Timor Oriental	2016
Tanzania	2016	Vietnam	2016
Bahamas	2017	Líbano	2017
Malaui	2017	Vanuatu	2017
Fiji	2018	San Cristóbal y Nieves	2018
Marruecos	2018	Seychelles	2018

1.3.1. En México

Se dice que el derecho a la información no nació en 1977; sino que se remonta desde épocas de la independencia. Sin embargo, este derecho estuvo íntimamente ligado a los derechos de expresión, de escribir y de publicar.

> Tal como lo documenta Jorge Carpizo, los Elementos Constitucionales de 1811, en su artículo 29, establecen la libertad de imprenta en temas científicos y políticos con fines ilustrativos. De las libertades de expresión e imprenta se ocuparon expresamente los artículos 371 de la constitución de Cádiz de 1812, el 49 de la de Apatzingán de 1814, el 31 del Acta Constitutiva de la Federación Mexicana de 1824, el 50 de la Constitución Federal de 1836, el 9, 10, 11 y 12 de las Bases Orgánicas de 1843 y el 6 y 7 de la Constitución de 1857, predominando el pensamiento de que la libertad supine: libertad de pensar, hablar, escribir, imprimir y hacer todo aquello que no ofendiese los derechos de los demás. Hasta 1867 se puede generalizar que se reconoció y protegió la libertad de expresión y sus manifestaciones más importantes, se prohibió la censura previa en varios documentos constitucionales, las libertades debían ser compatibles con otras como la vida privada, los derechos de terceros, etcétera, y que había una remisión general a leyes específicas para la reglamentación de las libertades y derechos. *En los artículos 6 y 7 de la Constitución de 1857 quedaron plasmadas estas ideas, ratificadas y vigentes en los mismos artículos constitucionales de la actual Constitución de 1917.*[103]

Desde el punto de vista contemporáneo, se puede encontrar en la llamada reforma política de 1977 cuando fue presidente José López Portillo y Pacheco, en ese año se reformaron los artículos 6o., 18, 41, 51, 52, 53, 54, 55, 60, 61, 65, 70, 73, 74, 76, 93, 97 y 115 constitucionales; sin embargo, para efectos de este trabajo solo me ocuparé del artículo 6°.

La reforma al artículo 6° constitucional se publicó en el Diario Oficial de la Federación el martes 06 de diciembre de 1977 en los siguientes términos:

> ARTÍCULO SEGUNDO.- Se modifica el artículo 6º, en la forma que a continuación se indica:
>
> "ARTÍCULO 6º.- La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, lo derechos de tercero, provoque algún delito o perturbe el orden público; el derecho a la información será garantizado por el Estado."

Se dice que esta forma fue más un derecho a la información que debían de garantizar los partidos políticos; es decir, era una garantía individual que se agotaba en el ámbito político -electoral. Esta parte se deduce de lo establecido por la Suprema Corte de Justicia de la Nación (SCJN) en los siguientes términos:

> INFORMACION. DERECHO A LA, ESTABLECIDO POR EL ARTICULO 6o. DE LA CONSTITUCION FEDERAL. La adición al artículo 6o. constitucional en el sentido de que el derecho a la información será garantizado por el Estado, se produjo con motivo de la iniciativa presidencial de cinco de octubre de mil novecientos setenta y siete, así como del dictamen de las Comisiones Unidas de Estudios Legislativos y Primera de Puntos Constitucionales de la

[103] Gamboa Montejano, Claudia, *Transparencia y Acceso a la Información Pública. Estudio de Antecedentes, Marco Jurídico Actual, Derecho Comparado de Diversos Países y de las Entidades Federativas, y de las iniciativas Presentadas en el Tema*, [en línea] México, CDDHCU. 2007, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *http://www.diputados.gob.mx/sedia/sia/spi/SPI-ISS-03-07.pdf* p. 6.

Cámara de Diputados de las que se desprende que: a) Que el derecho a la información es una garantía social, correlativa a la libertad de expresión, que se instituyó con motivo de la llamada "Reforma Política", y que consiste en que el Estado permita el que, a través de los diversos medios de comunicación, se manifieste de manera regular la diversidad de opiniones de los partidos políticos. b) Que la definición precisa del derecho a la información queda a la legislación secundaria; y c) Que no se pretendió establecer una garantía individual consistente en que cualquier gobernado, en el momento en que lo estime oportuno, solicite y obtenga de órganos del Estado determinada información. Ahora bien, respecto del último inciso no significa que las autoridades queden eximidas de su obligación constitucional de informar en la forma y términos que establezca la legislación secundaria; pero tampoco supone que los gobernados tengan un derecho frente al Estado para obtener información en los casos y a través de sistemas no previstos en las normas relativas, es decir, el derecho a la información no crea en favor del particular la facultad de elegir arbitrariamente la vía mediante la cual pide conocer ciertos datos de la actividad realizada por las autoridades, sino que esa facultad debe ejercerse por el medio que al respecto se señale legalmente.[104]

La tesis anterior derivó de un precedente judicial que en su parte sustantiva se determinó lo siguiente:

INFORMACION. DERECHO A LA, ESTABLECIDO POR EL ARTICULO 6o. DE LA CONSTITUCION FEDERAL.
AMPARO EN REVISION 10556/83. IGNACIO BURGOA ORIHUELA.
RESULTANDO:

PRIMERO.- Por escrito presentado el veintinueve de agosto de mil novecientos ochenta y tres ante la Oficialía de Partes Común a los Juzgados de Distrito en Materia Administrativa en el Distrito Federal, Ignacio Burgoa Orihuela, por su propio derecho, ocurrió en demanda de amparo en contra de la autoridad y por el acto que a continuación se precisan: "C. Autoridad responsable: C. Secretario de Hacienda y Crédito Público. D. Acto reclamado: El acuerdo negativo fechado el 12 de agosto de 1983 y que lleva el número 101-551, por medio del cual el C. Secretario de Hacienda y Crédito Público se rehusó a proporcionarme los informes que le solicité en mi escrito que ante dicho funcionario presenté el día 31 de enero del año en curso, en relación con los empréstitos que aumentaron en la cantidad de 37,600 millones de dólares la deuda externa de México durante el gobierno que presidió José López Portillo. Los informes por mí solicitados en el mencionado ocurso versan sobre los siguientes puntos: a). Monto y vencimiento de cada uno de los empréstitos públicos que con cargo al crédito de la nación se contrajeron en favor de bancos y gobiernos extranjeros; b). Indicación de las entidades extranjeras acreedoras de México; c). Determinación de los documentos en que se hayan hecho constar tales empréstitos públicos, con mención de los nombres de los funcionarios del sexenio próximo anterior que en nombre de México los

[104] Tesis: 2a. I/92, Semanario Judicial de la Federación, Octava Época, Tomo X, agosto de 1992, página 44.

firmaron; d). Indicación de si los mencionados empréstitos públicos se concertaron por orden, autorización o consentimiento del expresidente José López Portillo; e). Indicación de la aplicación que se hizo del dinero nacional proveniente de dichos empréstitos públicos; f). Indicación de las dependencias oficiales o de las entidades paraestatales a las que se haya entregado o acreditado el monto de los multicitados empréstitos; y g). Indicación de las obras que se hubiesen ejecutado para beneficio del pueblo mexicano con el dinero procedente de tales empréstitos públicos. Es evidente que el acuerdo negativo que impugno lo atribuyo al secretario de Estado responsable." […]

Tanto de la iniciativa como del dictamen aludidos se desprende lo siguiente:

a) Que el derecho a la información es una garantía social, correlativa a la libertad de expresión, que se instituyó con motivo de la llamada "reforma política", y que consiste en que el Estado permita el que, a través de los diversos medios de comunicación, se manifieste de manera regular la diversidad de opiniones de los partidos políticos.

b) Que la definición precisa del derecho a la información queda a la legislación secundaria; y

c) Que no se pretendió establecer una garantía individual consistente en que cualquier gobernado, en el momento en que lo estime oportuno, solicite y obtenga de órganos del Estado determinada información.

Esto no quiere decir que las autoridades se eximan de su obligación constitucional y legal de informar en la forma y términos en que la Constitución y la ley lo establezcan, pero tampoco supone que los gobernados tengan un derecho frente al Estado para obtener información en los casos y a través de sistemas no previstos en las normas relativas.

En efecto, como se ha señalado, el derecho a la información no crea en favor del quejoso la facultad de elegir arbitrariamente la vía mediante la cual pide conocer ciertos datos de la actividad realizada por las autoridades, sino que esa facultad debe adoptar el medio que al respecto se señale legalmente y, además, como se ha precisado, no es a través de un particular que la Secretaría de Hacienda y Crédito Público debe cumplir con el referido segundo párrafo del artículo 27 de la Ley General de la Deuda Pública. […]

Por lo expuesto y fundado y con apoyo, además, en los artículos 86, 88, 90, 91 y demás relativos de la Ley de Amparo, se resuelve:

PRIMERO.- Se confirma la sentencia recurrida.

SEGUNDO.- La Justicia de la Unión no ampara ni protege a Ignacio Burgoa Orihuela contra la autoridad y por el acto que se precisan en el resultando primero de esta resolución.[105]

[105] Precedente AMPARO EN REVISIÓN 10556/83 Octava Época Fuente: Semanario Judicial de la Federación.
Tomo X, Octubre de 1992, página 71 Instancia: Segunda Sala

A manera de paréntesis, cabe resaltar que esta tesis derivó de un amparo que en su momento interpuso un destacadísimo maestro de esta Facultad, el Dr. Ignacio Burgoa a quién como se pudo apreciar le fue negado dicho amparo.
Otro momento importante fue el muy mencionado incidente de Aguas Blancas, en Guerrero donde hubo una lamentable pérdida de 17 personas. Con motivo de este acontecimiento la SCJN ejerció su facultad de atracción en términos de la vigencia del artículo 97 constitucional y donde derivó el siguiente criterio:

> GARANTIAS INDIVIDUALES (DERECHO A LA INFORMACION). VIOLACION GRAVE PREVISTA EN EL SEGUNDO PARRAFO DEL ARTICULO 97 CONSTITUCIONAL. LA CONFIGURA EL INTENTO DE LOGRAR LA IMPUNIDAD DE LAS AUTORIDADES QUE ACTUAN DENTRO DE UNA CULTURA DEL ENGAÑO, DE LA MAQUINACION Y DEL OCULTAMIENTO, POR INFRINGIR EL ARTICULO 6o. TAMBIEN CONSTITUCIONAL.[106]
>
> El artículo 6o. constitucional, in fine, establece que "el derecho a la información será garantizado por el Estado". Del análisis de los diversos elementos que concurrieron en su creación se deduce que esa garantía se encuentra estrechamente vinculada con el respeto de la verdad. Tal derecho es, por tanto, básico para el mejoramiento de una conciencia ciudadana que contribuirá a que ésta sea más enterada, lo cual es esencial para el progreso de nuestra sociedad. Si las autoridades públicas, elegidas o designadas para servir y defender a la sociedad, asumen ante ésta actitudes que permitan atribuirles conductas faltas de ética, al entregar a la comunidad una información manipulada, incompleta, condicionada a intereses de grupos o personas, que le vede la posibilidad de conocer la verdad para poder participar libremente en la formación de la voluntad general, incurren en violación grave a las garantías individuales en términos del artículo 97 constitucional, segundo párrafo, pues su proceder conlleva a considerar que existe en ellas la propensión de incorporar a nuestra vida política, lo que podríamos llamar la cultura del engaño, de la maquinación y de la ocultación, en lugar de enfrentar la verdad y tomar acciones rápidas y eficaces para llegar a ésta y hacerla del conocimiento de los gobernados.

Esta tesis sirvió como base para otra tesis (Valga la redundancia), donde la SCJN amplía la visión en cuanto al alcance y naturaleza del derecho a la información en los siguientes términos:

> DERECHO A LA INFORMACIÓN. LA SUPREMA CORTE INTERPRETÓ ORIGINALMENTE EL ARTÍCULO 6o. CONSTITUCIONAL COMO GARANTÍA DE PARTIDOS POLÍTICOS, AMPLIANDO POSTERIORMENTE ESE CONCEPTO A GARANTÍA INDIVIDUAL Y A OBLIGACIÓN DEL ESTADO A INFORMAR VERAZMENTE.[107]

https://sjf2.scjn.gob.mx/detalle/ejecutoria/291

[106] Tesis: P. LXXXIX/96, Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo III, junio de 1996, p. 513.

[107] Tesis: P. XLV/2000, Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo XI, abril de 2000, p. 72.

> Inicialmente, la Suprema Corte estableció que el derecho a la información instituido en el último párrafo del artículo 6o. constitucional, adicionado mediante reforma publicada el 6 de diciembre de 1977, estaba limitado por la iniciativa de reformas y los dictámenes legislativos correspondientes, a constituir, solamente, una garantía electoral subsumida dentro de la reforma política de esa época, que obligaba al Estado a permitir que los partidos políticos expusieran ordinariamente sus programas, idearios, plataformas y demás características inherentes a tales agrupaciones, a través de los medios masivos de comunicación (Semanario Judicial de la Federación, Octava Época, 2a. Sala, Tomo X, agosto 1992, p. 44). Posteriormente, en resolución cuya tesis LXXXIX/96 aparece publicada en el Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo III, junio 1996, p. 513, este Tribunal Pleno amplió los alcances de la referida garantía al establecer que el derecho a la información, estrechamente vinculado con el derecho a conocer la verdad, exige que las autoridades se abstengan de dar a la comunidad información manipulada, incompleta o falsa, so pena de incurrir en violación grave a las garantías individuales en términos del artículo 97 constitucional. A través de otros casos, resueltos tanto en la Segunda Sala (AR. 2137/93, fallado el 10 de enero de 1997), como en el Pleno (AR. 3137/98, fallado el 2 de diciembre de 1999), la Suprema Corte ha ampliado la comprensión de ese derecho entendiéndolo, también, como garantía individual, limitada como es lógico, por los intereses nacionales y los de la sociedad, así como por el respeto a los derechos de tercero.

De esta forma, el derecho a la información en México transitó de ser una prerrogativa de los partidos políticos, para transmitir sus propuestas a través de los medios de comunicación, a erigirse como una garantía exigible al Estado con la finalidad de que éste proporcione información veraz, completa y objetiva a la sociedad."[108]

Para 2002, se emite la primera Ley de Transparencia y Acceso a la Información Pública Gubernamental (LGTAIPG), misma que fue aprobada en la cámara de senadores el 30 de abril de 2002 por 86 votos en lo general. Esta Ley fue publicada en el Diario Oficial de la Federación el 11 de junio de 2002 bajo la presidencia de Vicente Fox Quesada.

Un año más tarde, el 11 de junio de 2003 se publicó en el DOF el Reglamento de la Ley federal de Transparencia y Acceso a la Información Pública Gubernamental.
Esta ley tuvo como objeto según su artículo 1°: proveer lo necesario para garantizar el acceso de toda persona a la información en posesión de los Poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal, y cualquier otra entidad federal.

Por lo anterior, fue necesario desarrollar diferentes instrumentos normativos de

[108] INAI, *Introducción a la Ley Federal de Transparencia y Acceso a la Información Pública. Manual del Participante*, [en línea], México, INAI, 2016, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.sep.gob.mx/work/models/sep1/Resource/18094/4/images/m_ilftaip.pdf* p. 25

otros sujetos obligados por esta ley para el cumplimiento de las obligaciones de transparencia y acceso a la información pública gubernamental, tal como se aprecia en el siguiente cuadro[109]:

PODER LEGISLATIVO	
Cámara de Diputados	Decreto por el que se expide el Reglamento para la Transparencia y el Acceso a la Información Pública de la H. Cámara de Diputados. Acuerdo de la Mesa Directiva por el que se Establecen los Criterios de Clasificación, Desclasificación y Custodia de la Información Reservada y Confidencial
Senado de la República	Acuerdo Parlamentario para la Aplicación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental en la Cámara de Senadores
Auditoria Superior de la Federación	Acuerdo por el que se Establece la Integración y Funcionamiento del Comité de Información de la Auditoría Superior de la Federación

PODER JUDICIAL	
Suprema Corte de Justicia de la Nación	Reglamento de la Suprema Corte de Justicia de la Nación y del Consejo de la Judicatura Federal para la Aplicación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental
	Acuerdo Número 9/2003 del veintisiete de mayo de dos mil tres, del Tribunal Pleno de la Suprema Corte de Justicia de la Nación, que Establece los Órganos, Criterios y procedimientos Institucionales, para la Transparencia y Acceso a la Información Pública de este Alto Tribunal

[109] Basado en Martínez Bejarano, María Eugenia *Coord*, *Compilación Jurídica de los otros sujetos obligados por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental*, [en línea] México, IIJ-INAI, 2005, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://biblio.juridicas.unam.mx/bjv/detalle-libro/5181-compilacion-juridica-de-los-otros-sujetos-obligados-por-la-ley-federal-de-transparencia-y-acceso-a-la-informacion-publica-gubernamental*

SCJN	Acuerdo Número 13/2003, de dos de diciembre de dos mil tres, del Tribunal Pleno de la Suprema Corte de Justicia de la Nación, que Modifica el Diverso 9/2003, del veintisiete de mayo de dos mil tres, del propio Pleno, que Establece los Órganos, Criterios y Procedimientos Institucionales, para la Transparencia y Acceso a la Información Pública de este Alto Tribunal
	Lineamientos de la Comisión de Transparencia y Acceso a la Información de la Suprema Corte de Justicia de la Nación, del dos de junio de dos mil tres, relativos a la Organización, Catalogación, Clasificación y Conservación de la Documentación de este Alto Tribunal
Tribunal Electoral del Poder Judicial de la Federación	Acuerdo General que Establece los Órganos, Criterios y Procedimientos Institucionales para la Transparencia y Acceso a la Información Pública del Tribunal Electoral del Poder Judicial de la Federación
Consejo de la Judicatura Federal	Acuerdo General 30/2003 del Pleno del Consejo de la Judicatura Federal, que Establece los Órganos, Criterios y Procedimientos Institucionales para la Transparencia y Acceso a la Información Pública para este Órgano del Poder Judicial de la Federación, los Tribunales de Circuito y los Juzgados de Distrito
	Lineamientos de la Comisión para la Transparencia y Acceso a la Información del Consejo de la Judicatura Federal, de los Tribunales de Circuito y los Juzgados de Distrito, relativos a los Criterios de Clasificación y Conservación de la Información Reservada o Confidencial, para este Órgano del Poder Judicial de la Federación, los Tribunales de Circuito y los Juzgados de Distrito

ÓRGANOS CONSTITUCIONALES AUTÓNOMOS	
Universidades e instituciones de Educación Superior con Autonomía Legal	
Universidad Nacional Autónoma de México	Acuerdo para la Transparencia y Acceso a la Información en la Universidad Nacional Autónoma de México
Universidad Autónoma Metropolitana	Acuerdo 08/2003 del Rector General mediante el cual se emiten los Lineamientos para el Acceso a la Información de la Universidad Autónoma Metropolitana y se Crea la Coordinación de Enlace y Acceso a la Información Universitaria
	Lineamientos para el Acceso a la Información de la Universidad Autónoma Metropolitana
Universidad Autónoma Chapingo	Acuerdo para la Transparencia y Acceso a la Información en la Universidad Autónoma Chapingo
	Lineamientos para el Acceso a la Información de la Universidad Autónoma Chapingo
	FE DE ERRATAS: Relativo al Acuerdo para la Transparencia y Acceso a la Información en la Universidad Autónoma Chapingo
Banco de México	Reglamento del Banco de México relativo a La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental
	Reglas de Funcionamiento del Comité de Información del Banco de México
	Criterios del Comité de Información para Clasificar la Información en Reservada y Confidencial de Conformidad con la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental
Instituto Federal Electoral	Acuerdo del Consejo General por el que se aprueba el Reglamento del Instituto Federal Electoral en Materia de Transparencia y Acceso a la Información Pública. Cg110/2003
	Lineamientos para la Celebración de Sesiones del Comité de Información del

	Instituto Federal Electoral
	Acuerdo de la Comisión del Consejo para la Transparencia y Acceso a la Información por el que se Aprueban Criterios Operativos Relativos a los Recursos de Revisión y Reconsideración
Comisión Nacional de los Derechos Humanos	Acuerdo del Consejo Consultivo de la Comisión Nacional de los Derechos Humanos por el que se aprueba el Reglamento de Transparencia y Acceso a la Información de la Comisión Nacional de los Derechos Humanos

TRIBUNALES ADMINISTRATIVOS	
Tribunal Federal de Justicia Fiscal y Administrativa	Acuerdo G/18/2003, mediante el cual se expide el Reglamento para dar Cumplimiento a la Ley de Transparencia y Acceso a la Información Pública Gubernamental
Tribunal Federal de Conciliación y Arbitraje	Reglamento de Transparencia y Acceso a la Información del Tribunal Federal de Conciliación y Arbitraje
Tribunal Superior Agrario	Reglamento de los Tribunales Agrarios para la Transparencia y Acceso a la Información

Si bien ya se tenía un primer avance serio en materia de combate a la opacidad o dicho en positivo en favor de la transparencia, rendición de cuentas y acceso a la información, aún faltaba un camino largo por recorrer. De esta forma, para 2006, las Comisiones Unidas de Puntos Constitucionales y de la Función Pública de la Cámara de Diputados sometieron el proyecto de decreto que reformaba el artículo 6º constitucional.

La iniciativa fue presentada por los entonces diputados Emilio Gamboa Patrón, Héctor Larios Córdova, Javier González Garza, Gloria Lavara Mejía, Alejandro Chanona Burguete, Ricardo Cantú Garza, Miguel Ángel Jiménez Godínez y Aída Marina Arvizu Rivas; y fue turnada para su estudio y elaboración del dictamen correspondiente a la Comisión de Puntos Constitucionales.

En el punto **III. Antecedentes de la Iniciativa** se pueden recoger algunas ideas:

> La promulgación y entrada en vigor de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental es una de las adquisiciones democráticas más importantes de México en los años recientes. Su vigencia ha contribuido a la apertura del Estado, al conocimiento público de los asuntos

importantes para la nación, ha puesto en manos de los ciudadanos una gran cantidad y variedad de datos, cifras y documentos para la toma de sus propias decisiones y ha ayudado a remover inercias gubernamentales indeseables como el secretismo, el patrimonialismo, la corrupción y la discrecionalidad.

Esa ley se ha constituido en una poderosa palanca para la democratización del estado, y su ejemplo ha impactado en otras áreas, instituciones y niveles de gobierno en todo el país, difundiendo una nueva cultura acerca de "lo público" entre los ciudadanos y los funcionarios y, como nunca antes, las instituciones difunden, publican y hacen accesible una gran cantidad de información relevante sobre sus actividades. A partir de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y de las leyes equivalentes aprobadas por el resto de los Estados de la República, se han establecido condiciones que mejoran, aunque con deficiencias aún importantes, el derecho de los mexicanos de acceder a documentos que testimonian la acción gubernamental y el uso de los recursos públicos. […]

Desde el año 2002, el país ha cursado una larga ruta de construcción jurídica e institucional en todos los Estados de la Federación.

Sin embargo, el desarrollo del derecho de acceso a la información no ha estado exento de problemas, resistencias y deformaciones. Quizás, la dificultad más importante es la heterogeneidad con la que se ha legislado y con la que se ejerce hoy mismo en las entidades y en las instituciones de la República, una diversidad perjudicial para la práctica de un derecho que es fundamental.

Esta iniciativa reconoce tres grandes antecedentes:

NOMBRE	CARACTERÍSTICAS	ASPECTOS IMPORTANTES
Declaración de Guadalajara	Primer Foro Nacional de Transparencia Local Realizada en Guadalajara 22 de noviembre de 2005	Se propone una reforma constitucional que incorpore al texto fundamental el derecho de acceso a la información pública y los requisitos mínimos a cumplir en y por toda la República, a saber: 1) Otorgar a todo mexicano y a toda persona los mismos derechos: sujetar las leyes a los principios de máxima publicidad y gratuidad. 2) Facilitar al máximo la solicitud de información sin condicionantes artificiales, como la exigencia de demostrar personalidad, firma, identificación o interés jurídico. 3) Poner a disposición del público todas las modalidades para

NOMBRE	CARACTERÍSTICAS	ASPECTOS IMPORTANTES
		tramitar solicitudes de información, incluyendo las herramientas electrónicas. 4) Crear instancias profesionales, autónomas e imparciales para generar una cultura de transparencia y garantizar el acceso a la información en caso de controversia. 5) Establecer sanciones para los funcionarios que nieguen dolosamente la información. 6) La obligación de todos los órganos públicos de transparentar los principales indicadores de gestión. 7) Asegurar la protección de los datos personales.
XXVII Reunión ordinaria de la Conferencia Nacional de Gobernadores (CONAGO)	XXVII Reunión Ordinaria de la Conferencia Nacional de Gobernadores, Celebrada en Guanajuato durante el mes de marzo de 2006.	El entonces Instituto Federal de Acceso a la Información Pública (IFAI) tuvo ocasión de exponer lo siguiente: "En México el acceso a la información fue engendrado por el consenso de todos los partidos políticos. La Ley Federal de Transparencia tuvo un nacimiento unánime. Este hecho explica su fortaleza y también, su expansión a lo largo y ancho de la República. Aunque no existía ninguna obligación expresa, hoy, 28 Estados de la República tienen en marcha una ley de transparencia y cuatro más ya la discuten en sus Congresos, precisamente porque estas leyes y este derecho no son el monopolio de ningún partido, ni de ningún gobierno, sino el síntoma de un acuerdo verdaderamente nacional.
La Iniciativa de Chihuahua	Realizada en el Segundo Congreso de Transparencia	De manera particular, los principios que en la materia se proponen son los siguientes:

NOMBRE	CARACTERÍSTICAS	ASPECTOS IMPORTANTES
	Local en Chihuahua 10 de noviembre de 2006 El documento fue firmado por los Gobernadores de Aguascalientes, Chihuahua y Zacatecas y se sumaron el Gobernador del Estado de Veracruz, Fidel Herrera, y el entonces Jefe de Gobierno del Distrito Federal, Alejandro Encinas	a) Principio de publicidad sujeta a excepciones por causa de interés público. b) Acceso a la información de todos los órganos del estado y los partidos políticos. c) Un procedimiento expedito para el acceso a la información. d) Un procedimiento expedito para el acceso y rectificación de los datos personales. e) Un procedimiento de revisión de las decisiones desfavorables ante un organismo especializado e imparcial que goce de autonomía operativa, presupuestal y de decisión. f) Prueba de daño y de interés público. g) Sanciones administrativas para los servidores públicos. h) Obligación de proporcionar información. i) La existencia de archivos administrativos actualizados y confiables. j) Protección de la vida privada.

En el análisis de la iniciativa se desarrollaron varios principios (primeras tres fracciones) y bases operativas (fracciones IV a VII):

I. Contienen el principio básico de la reforma, toda la información en posesión de órganos del estado mexicano es pública.
   a. Se rompe con las concepciones patrimonialistas o cerradas de la información.
   b. Se precisan quienes serán los sujetos obligados.
   c. La excepción al principio de máxima publicidad, deben ser aplicadas de manera restrictiva y limitada.

II. Establece una segunda limitación al derecho de acceso a la información.
   a. Se refiere a la protección de la vida privada y de los datos personales.
   b. No debe confundirse la vida privada con los datos personales.

i. La primera se refiere al ámbito de privacidad de las personas respecto de la intervención tanto del estado como de otros particulares.
ii. Los datos personales, en cambio, son una expresión de la privacidad

III. El ejercicio del derecho de acceso a la información, y de acceso y rectificación de datos personales, no pueden estar condicionados.
   a. Establece el principio de gratuidad tanto en el ejercicio del derecho de acceso a la información como en el de acceso o rectificación de los datos personales.

IV. Desarrollo de mecanismos de acceso que permitan a cualquier persona realizar y obtener de manera expedita el acceso a la información, a sus datos personales o la rectificación de estos últimos
   a. Establecimiento de órganos garantes.

V. Política de estado plenamente comprometida con la transparencia y la rendición de cuentas.
   a. El derecho de acceso a la información está íntimamente vinculado con los conceptos de transparencia y rendición de cuentas, pero no deben confundirse.
   b. Sistema de círculos concéntricos.
      i. Al centro se encuentra el “derecho de acceso a la información” que es un derecho fundamental y supone la potestad del ciudadano de solicitar información a las autoridades y la obligación correlativa de éstas de responderle.
      ii. El segundo círculo corresponde a la transparencia, que incluye el derecho de acceso, pero que tiene un contenido más amplio pues implica una política pública que busca maximizar el uso público de la información y que debería proveer las razones que justifican una acción o decisión determinadas.
      iii. Un tercer círculo, más amplio, es el de la rendición de cuentas. (Incluye a la transparencia, pero contiene una dimensión adicional, que es la sanción como un elemento constitutivo)

VI. Las leyes determinarán la manera en que los sujetos obligados deberán hacer pública la información relativa a los recursos públicos que entreguen a personas físicas o morales.

VII. La inobservancia a las disposiciones contenidas en las leyes en la materia, será sancionada en los términos que dispongan los ordenamientos correspondientes.

Una vez aprobado en la Cámara de Diputados, paso al Senado en abril de 2007, donde las comisiones unidas de puntos constitucionales y de estudios legislativos emitieron un dictamen donde se destacan los objetivos esenciales señalados por la cámara de Diputados y presenta 3 argumentos fundamentales:

1. Heterogeneidad Indeseable.

2. Cuestión Municipal.
3. Partidos Políticos.[110]

Después de que fue aprobada esta reforma, el 20 de julio de 2007 se publicó en el DOF el decreto por el que se adiciona un segundo párrafo con siete fracciones al Artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos.

> Artículo Único.- Se adiciona un segundo párrafo con siete fracciones al Artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, para quedar como sigue:
>
> Artículo 6o.- ...
>
> 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:
>
> I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad.
>
> 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.
>
> IV. Se establecerán mecanismos de acceso a la información y procedimientos de revisión expeditos. Estos procedimientos se sustanciarán ante órganos u organismos especializados e imparciales, y con autonomía operativa, de gestión y de decisión.
>
> V. Los sujetos obligados deberán preservar sus documentos en archivos administrativos actualizados y publicarán a través de los medios electrónicos disponibles, la información completa y actualizada sobre sus indicadores de gestión y el ejercicio de los recursos públicos.
>
> VI. Las leyes determinarán la manera en que los sujetos obligados deberán hacer pública la información relativa a los recursos públicos que entreguen a personas físicas o morales.
>
> VII. La inobservancia a las disposiciones en materia de acceso a la información pública será sancionada en los términos que dispongan las leyes.

[110] INAI, *Reforma al artículo 6° constitucional que establece el acceso a la información pública como un derecho fundamental de los mexicanos*, México, INAI, 2007, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/ModificacionArt6.pdf* pp. 7-48.

Sin embargo; esta no sería la última reforma constitucional. La siguiente reforma constitucional fue publicada en el DOF el 11 de junio de 2013 y aunque fue diseñada principalmente en materia de Telecomunicaciones también hubo modificaciones al artículo 6° en el siguiente sentido:

> Artículo 6o. La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida privada o los derechos de terceros, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.
>
> Toda persona tiene derecho al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión.
>
> El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios.
>
> Para efectos de lo dispuesto en el presente artículo se observará lo siguiente:
>
> A. 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:
> I. a VII. ...

En 2014, se presentó otra gran reforma en materia de transparencia. “Esta reforma constitucional obliga a las autoridades de los tres órdenes de gobierno a implementar mecanismos que garanticen el acceso a la información, así como a crear organismos autónomos en cada una de las entidades federativas que aseguren la máxima transparencia en el uso de la información, a fin de que ésta esté disponible para cualquier ciudadano.”[111]

Dicha reforma constitucional se sustentó en tres ejes principales:

1) Fortalecimiento del derecho de acceso a la información pública.
2) La consolidación de un sistema nacional de transparencia.
3) El establecimiento de nuevas facultades para el entonces IFAI.

Esta reforma se publicó en el DOF el 07 de febrero de 2014 en el siguiente sentido:

> Artículo 6o. ...
> ...

[111] s/a, *Reforma en Materia de Transparencia*, [en línea], México, Gobierno de la República, 2014, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.gob.mx/cms/uploads/attachment/file/66464/13_Transparencia.pdf* p. 3.

A. 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:

I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público y seguridad nacional, en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad. Los sujetos obligados deberán documentar todo acto que derive del ejercicio de sus facultades, competencias o funciones, la ley determinará los supuestos específicos bajo los cuales procederá la declaración de inexistencia de la información.

II. y III. ...

IV. Se establecerán mecanismos de acceso a la información y procedimientos de revisión expeditos que se sustanciarán ante los organismos autónomos especializados e imparciales que establece esta Constitución.

V. Los sujetos obligados deberán preservar sus documentos en archivos administrativos actualizados y publicarán, a través de los medios electrónicos disponibles, la información completa y actualizada sobre el ejercicio de los recursos públicos y los indicadores que permitan rendir cuenta del cumplimiento de sus objetivos y de los resultados obtenidos.

VI. y VII. ...

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 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.

En su funcionamiento se regirá por los principios de certeza, legalidad, independencia, imparcialidad, eficacia, objetividad, profesionalismo, transparencia y máxima publicidad.

El organismo garante tiene competencia para conocer de 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 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; 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. También conocerá de los recursos que interpongan los particulares respecto de las resoluciones de los organismos autónomos especializados de los estados y el Distrito Federal que determinen la reserva, confidencialidad, inexistencia o negativa de la información, en los términos que establezca la ley.
El organismo garante federal de oficio o a petición fundada del organismo garante equivalente del estado o del Distrito Federal, podrá conocer de los recursos de revisión que por su interés y trascendencia así lo ameriten.

La ley establecerá aquella información que se considere reservada o confidencial.

Las resoluciones del organismo garante son vinculatorias, definitivas e inatacables para los sujetos obligados. El Consejero Jurídico del Gobierno podrá interponer recurso de revisión ante la Suprema Corte de Justicia de la Nación en los términos que establezca la ley, sólo en el caso que dichas resoluciones puedan poner en peligro la seguridad nacional conforme a la ley de la materia.

El organismo garante se integra por siete comisionados. Para su nombramiento, la Cámara de Senadores, previa realización de una amplia consulta a la sociedad, a propuesta de los grupos parlamentarios, con el voto de las dos terceras partes de los miembros presentes, nombrará al comisionado que deba cubrir la vacante, siguiendo el proceso establecido en la ley. El nombramiento podrá ser objetado por el Presidente de la República en un plazo de diez días hábiles. Si el Presidente de la República no objetara el nombramiento dentro de dicho plazo, ocupará el cargo de comisionado la persona nombrada por el Senado de la República.

En caso de que el Presidente de la República objetara el nombramiento, la Cámara de Senadores nombrará una nueva propuesta, en los términos del párrafo anterior, pero con una votación de las tres quintas partes de los miembros presentes. Si este segundo nombramiento fuera objetado, la Cámara de Senadores, en los términos del párrafo anterior, con la votación de las tres quintas partes de los miembros presentes, designará al comisionado que ocupará la vacante.

Los comisionados durarán en su encargo siete años y deberán cumplir con los requisitos previstos en las fracciones I, II, IV, V y VI del artículo 95 de esta Constitución, no podrán tener otro empleo, cargo o comisión, con excepción de los no remunerados en instituciones docentes, científicas o de beneficencia, sólo podrán ser removidos de su cargo en los términos del Título Cuarto de esta Constitución y serán sujetos de juicio político.

En la conformación del organismo garante se procurará la equidad de género.

El comisionado presidente será designado por los propios comisionados, mediante voto secreto, por un periodo de tres años, con posibilidad de ser reelecto por un periodo igual; estará obligado a rendir un informe anual ante el Senado, en la fecha y en los términos que disponga la ley.

El organismo garante tendrá un Consejo Consultivo, integrado por diez consejeros, que serán elegidos por el voto de las dos terceras partes de los miembros presentes de la Cámara de Senadores. La ley determinará los procedimientos a seguir para la presentación de las propuestas por la propia Cámara. Anualmente serán sustituidos los dos consejeros de mayor antigüedad en el cargo, salvo que fuesen propuestos y ratificados para un segundo periodo.

La ley establecerá las medidas de apremio que podrá imponer el organismo garante para asegurar el cumplimiento de sus decisiones.

Toda autoridad y servidor público estará obligado a coadyuvar con el organismo garante y sus integrantes para el buen desempeño de sus funciones.

El organismo garante coordinará sus acciones con la entidad de fiscalización superior de la Federación, con la entidad especializada en materia de archivos y con el organismo encargado de regular la captación, procesamiento y publicación de la información estadística y geográfica, así como con los organismos garantes de los estados y el Distrito Federal, con el objeto de fortalecer la rendición de cuentas del Estado Mexicano.

Asimismo, se establecieron nuevas facultades del Congreso de la Unión para legislar en la materia, lo cual quedó de la siguiente forma:

Artículo 73. ...

I. a XXIX-R. ...

XXIX-S. Para expedir las 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 niveles de gobierno.

XXIX-T. Para expedir la ley general que establezca la organización y administración homogénea de los archivos en los órdenes federal, estatal, del Distrito Federal y municipal, que determine las bases de organización y funcionamiento del Sistema Nacional de Archivos.

La última reforma constitucional al artículo 6° se publicó el 29 de enero de 2016 en materia de la reforma política de la Ciudad de México, ajustando el artículo en los siguientes términos:

Artículo 6o. ...

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:

I. a VII. ...

VIII. ...
El organismo garante tiene competencia para conocer de 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. También conocerá de 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.

El organismo garante federal, de oficio o a petición fundada del organismo garante equivalente de las entidades federativas, podrá conocer de los recursos de revisión que por su interés y trascendencia así lo ameriten. [...]

El organismo garante coordinará sus acciones con la Auditoría Superior de la Federación, con la entidad especializada en materia de archivos y con el organismo encargado de regular la captación, procesamiento y publicación de la información estadística y geográfica, así como con los organismos garantes de las entidades federativas, con el objeto de fortalecer la rendición de cuentas del Estado Mexicano.

Posteriormente, con fundamento en el mismo artículo Segundo Transitorio de la Reforma Constitucional, que estableció la obligación al Congreso de la Unión de reformar, entre otras normas, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y la Ley Federal de Datos Personales en Posesión de los Particulares; el 09 de mayo del año 2016 se publicó en el Diario Oficial de la Federación, la Ley Federal de Transparencia y Acceso a la Información Pública, la cual abrogó a la LFTAIPG del año 2002. Dicha Ley Federal entró en vigor el día 10 de mayo de 2016, es decir, al día siguiente de su publicación, de conformidad con su Primer Transitorio.

1.4. Aplicación de la Teoría General de Sistemas

Este punto consideré conveniente abordarlo porque las nuevas leyes generales tanto de Transparencia, como de Datos Personales establecen un sistema, el llamado Sistema Nacional de Transparencia (SNT).

Con esto, las leyes generales tienen como base el tener una concurrencia; es decir, que tanto la federación como las entidades federativas pueden regular sobre una misma materia.

Como se ha visto a lo largo de este trabajo en un principio la regulación de la materia versaba sobre facultades coincidentes, lo que generaba disparidades en la regulación de la materia y de los alcances de los órganos garantes.

Con la reforma constitucional de 2014, se crea un nuevo sistema de transparencia, el cual también se vincula con el sistema nacional anticorrupción; por lo que considero que estamos en presencia de un sistema de sistemas. Por ello se tomarán los estudios de Ludwig Von Bertalanffy y de Niklas Luhmann.

Sin embargo, antes de abordar a los autores arriba mencionados, primero tomaremos un pequeño glosario de definiciones aplicadas a la Teoría General de Sistemas o TGS.[112]

COMPLEJIDAD: Indica la cantidad de elementos de un sistema, sus potenciales interacciones (conectividad) y el número de estados posibles que se producen a través d estas (variabilidad indica el máximo de relaciones posibles: n!). Una versión más sofisticada de la TGS se funda en las nociones de diferencia de complejidad y variedad. Estos fenómenos fueron desarrollados por la cibernética y están asociados a los postulados de Ashby, donde se sugiere que el número de estados posibles que puede alcanzar el entorno es prácticamente infinito. Según esto, no habría sistema capaz de igualar tal variedad, puesto que si así fuera, la identidad, es decir su identidad, se diluiría.

DIFERENCIACIÓN: El desarrollo de un sistema implica su especialización funcional, es decir, procesos de elaboración de nuevos componentes. Bertalanffy señala que, durante el proceso de diferenciación, los organismos pasan por estados de heterogeneidad progresiva. Originalmente los sistemas están formados por partes totipotenciales, pero durante su desarrollo surge, a partir de la interacción dinámica de los componentes, un cierto orden que impone restricciones y especialización de estas partes con respecto al sistema, con lo cual pierden su potencialidad multifuncional. Lo anterior quiere decir que, en los procesos

[112] Osorio, Francisco, *et. al. La Nueva Teoría Social en Hispanoamérica. Introducción a la Teoría de sistemas Constructivista*, [en línea] México, UAEMex, Colección Pensamiento Universitario, Número 11, 2008. [fecha de consulta: 3 de diciembre de 2022] Disponible en: *http://ri.uaemex.mx/bitstream/handle/20.500.11799/3617/Nueva_teoria_social_en_Hispanoamerica_Osorio_Arnold.pdf?sequence=3* pp.35-46.

diferenciadores, las pautas globales difusas son reemplazadas por funciones especializadas.

ENTORNO: El entorno refiere al área de sucesos y condiciones que influyen sobre el comportamiento de un sistema. En lo que a complejidad se refiere, nunca un sistema puede igualarse con el entorno y seguir conservando su identidad. La única posibilidad de relación entre un sistema y su entorno implica que el primero debe absorber selectivamente aspectos de éste. Sin embargo, esta estrategia tiene la desventaja de especializar la selectividad del sistema respecto a su entorno, lo que disminuye su capacidad de reacción frente a los cambios externos. Esto último incide directamente en la aparición o desaparición de sistemas abiertos.

EQUIFINALIDAD: La equifinalidad indica la capacidad, demostrada por los sistemas abiertos, de llegar a un mismo fin partiendo de distintas condiciones iniciales. El proceso inverso, llegar a distintos fines desde un mismo punto de partida, se denomina multifinalidad. El fin en los sistemas abiertos refiere a el mantenimiento de un estado de equilibrio fluyente que implica, necesariamente, la importación de recursos energéticos, materiales o informativos provenientes del entorno. Con este marco de referencia, todos los sistemas son funcionalmente equivalentes, en tanto tienden al equilibrio y desarrollan sus mecanismos y operaciones con tal objeto.

EQUILIBRIO: Los estados de equilibrio pueden ser alcanzados en los sistemas abiertos por diversos caminos, esto se denomina equifinalidad y multifinalidad. El mantenimiento del equilibrio en sistemas abiertos implica necesariamente la importación de recursos provenientes del entorno. Estos recursos pueden consistir en flujos energéticos, materiales o informativos.

ESTRUCTURA: Las interrelaciones más o menos estables entre las partes o componentes de un sistema y que pueden ser identificadas en un momento dado, constituyen su estructura. Según Buckley, las clases particulares de interrelaciones, más o menos estables, de los componentes sistémicos constituyen su estructura particular en ese momento, alcanzando de tal modo una suerte de “totalidad” dotada de cierto grado de continuidad y de limitación.

FUNCIÓN Y SERVICIO: Se denomina función al output de un sistema que está dirigido a la conservación del sistema mayor en el que se encuentra inscrito. Servicios o prestaciones son los outputs de un sistema que van a servir de inputs a otros sistemas o subsistemas equivalentes.

HOMEOSTASIS: Este concepto está especialmente referido a los organismos vivos en tanto sistemas adaptables. Los procesos homeostáticos operan ante variaciones de las condiciones del entorno, corresponden a las compensaciones internas que sustituyen, bloquean o complementan estos cambios con el objeto de mantener invariante la estructura sistémica, es decir, hacia la conservación de su forma. La conservación de formas dinámicas o trayectorias se denomina *homeorrosis*

(sistemas cibernéticos).

INFORMACIÓN: Se pueden diferenciar las relaciones que establecen los sistemas abiertos de acuerdo a los distintos comportamientos que tienen las transferencias energéticas, materiales e informativas que componen sus intercambios. La información, que es la más importante de las corrientes de que disponen los sistemas complejos, opera *negentrópicamente* (no es una suma constante, pues agrega y no elimina), pues su comunicación no elimina la información del emisor o fuente. En términos formales, la cantidad de información que permanece en el sistema es igual a la información que existe más la que entra, es decir, hay una agregación neta en la entrada y la salida, pero no es eliminada la información del sistema. Mientras la energía y la materia son afectadas por la entropía, la información es especificidad e improbabilidad y por lo tanto revierte la entropía. La teoría de la información de Shannon y Weaver destaca el valor de la novedad en la información: un mensaje tiene mayor valor informático cuando su probabilidad es menor —"nevó en el desierto"— o cuando es más específico —"pesa 3.752 gramos"— o cuanto más probable es el mensaje, menos información contiene (Wiener).

INPUT / OUTPUT (modelo de): Los conceptos de input y output nos aproximan instrumentalmente al problema de los límites en los sistemas abiertos. Se dice que los sistemas que operan bajo esta modalidad son procesadores de entradas y elaboradores de salidas. Se denomina input a la importación de los recursos (energía, materia, información) que se requieren para dar inicio al ciclo de actividades del sistema. Se denomina output a las corrientes de salidas de un sistema y pueden diferenciarse según su destino en funciones o servicios.

INTERRELACIONES: Que un sistema sea abierto significa que establece intercambios permanentes con su entorno. Las relaciones entre los elementos de un sistema o entre éste y su entorno son vitales para la comprensión de los sistemas vivos, pues desde la conservación de las relaciones se explica su viabilidad. Los sistemas dependen de la importación, procesamiento e intercambio de energía, materia o información obtenida en sus entornos. A través de tales intercambios, que pueden ser reales o ideales, activos o latentes, naturales o artificiales, recíprocos o unidireccionales, determinan su equilibrio y continuidad. Varias distinciones se utilizan para identificar estos procesos: funciones, servicios, prestaciones, efectos recíprocos, asociaciones, interdependencias, comunicaciones, coherencia, conectividad, etc. Estas relaciones pueden como una red estructurada a través del esquema input / output.

LÍMITES: Los sistemas consisten en totalidades y, por lo tanto, son indivisibles como sistemas. Poseen partes y componentes, pero éstos son otras totalidades (emergencia). En algunos sistemas, sus límites coinciden con discontinuidades estructurales entre éstos y sus entornos, pero corrientemente la demarcación de los límites sistémicos queda en manos de un observador. En términos operacionales, puede decirse que la frontera del sistema es aquella línea que

separa al sistema de su entorno, definiendo lo que le pertenece y lo que queda fuera de él.

MODELO: Los modelos son construidos y diseñados por un observador que persigue identificar y mensurar relaciones sistémicas complejas. Todo sistema real tiene la posibilidad de ser representado en más de un modelo. La decisión, en este punto, depende tanto de los objetivos del modelador, como de su capacidad para distinguir las relaciones relevantes con relación a tales objetivos. La esencia de la modelística sistémica es la simplificación. El metamodelo sistémico más conocido es el esquema input-output.

NEGENTROPÍA/ ENTROPÍA: Estas distinciones provienen de los principios fundamentales de la termodinámica: la conservación de la energía y la entropía. El primero hace referencia a que la energía no se crea ni se destruye, sólo se transforma; el segundo refiere al cambio cualitativo e irreversible que sufre la energía cuando es sometida a un proceso físico y establece que la máxima probabilidad de los sistemas es su progresiva desorganización y, finalmente, su homogeneización con el entorno. Los sistemas cerrados están irremediablemente condenados a la desorganización. Desde el segundo principio de la termodinámica se establece que los procesos naturales tienden al aumento del grado de desorden conocido como entropía. En una definición más técnica, podemos entender a la entropía con un estado aleatorio de la energía que la hace no disponible para realizar trabajos. No obstante, hay sistemas que (al menos temporalmente) revierten esta tendencia al aumentar sus estados de organización. Específicamente, los sistemas vivos parecen contradecir esta ley al conservarse su organización en un estado de alta improbabilidad. Más aún, Bertalanffy señala que durante el proceso de diferenciación un organismo pasa por estados de heterogeneidad progresiva. Este fenómeno se explica porque los sistemas abiertos son capaces de importar energía y, así, de importar la entropía negativa o negentropía que les permite mantener un estado estable y altamente improbable de organización, e incluso desarrollar niveles más altos de organización e improbabilidad. Para el caso de los sistemas que operan información, Wiener establece que la entropía es el negativo de información, por lo tanto: a mayor información, menor entropía.

ORGANIZACIÓN: Wiener planteó que la organización debía concebirse como una interdependencia de distintas partes organizadas, pero una interdependencia que tiene grados. Ciertas interdependencias internas son más importantes que otras, lo cual equivale a decir que la interdependencia interna no es completa. Por lo cual, la organización sistémica se refiere al patrón de relaciones que definen los estados posibles (variabilidad) para un sistema determinado.

RELACIONES: Las relaciones internas y externas de los sistemas han tomado diversas denominaciones. Entre otras: efectos recíprocos, interrelaciones, organización, comunicaciones, flujos, prestaciones, asociaciones, intercambios, interdependencias, coherencias, etcétera. Las relaciones entre los elementos de un

sistema y su entorno son de vital importancia para la comprensión del comportamiento de sistemas vivos. Las relaciones pueden ser recíprocas o unidireccionales. Presentadas en un momento del sistema, las relaciones pueden ser observadas como una red estructurada bajo el esquema input-output.

SISTEMAS ABIERTOS: Se trata de sistemas que importan y procesan elementos (energía, materia, información) de sus entornos y esta es una característica propia de todos los sistemas vivos. Que un sistema sea abierto significa que establece intercambios permanentes con su entorno a través de los cuales determina su equilibrio, capacidad reproductiva o continuidad, es decir, su viabilidad.

SISTEMAS CERRADOS: Un sistema es cerrado cuando ningún elemento de afuera entra y ninguno sale del sistema. Estos sistemas alcanzan su estado máximo de equilibrio al igualarse con el medio. En ocasiones el concepto de sistema cerrado se aplica a sistemas que se comportan de una manera fija, rítmica o sin variaciones, como sería el caso de los circuitos cerrados.

SISTEMAS CIBERNÉTICOS: Son aquellos que disponen de dispositivos internos de autorregulación que reaccionan ante informaciones de cambios en el entorno, elaborando respuestas variables que contribuyen al cumplimiento de los fines instalados en el sistema.

SISTEMAS TRIVIALES Y SISTEMAS NO TRIVIALES: Las “máquinas triviales” son artefactos que responden con el mismo output cada vez que reciben un mismo input. No modifican su comportamiento con la experiencia. Las “máquinas no triviales” aparecen como erráticas e impredecibles. Frente a un mismo input pueden entregar outputs totalmente diferentes. Son sistemas cuyos estados internos cambian cada vez que computan un output, están totalmente determinados, sólo que nos resulta imposible predecir sus cambios de estado.

SISTEMAS (dinámica de) (J. W. Forrester): Comprende metodologías para la construcción de modelos de sistemas sociales, que establecen procedimientos y técnicas para el uso de lenguajes formalizados. Sus pasos son los siguientes:

a) Observación del comportamiento de un sistema real.
b) Identificación de los componentes y procesos fundamentales del mismo.
c) Identificación de las estructuras de retroalimentación que permiten explicar su comportamiento.
d) Construcción de un modelo formalizado sobre la base de la cuantificación de los atributos y sus relaciones.
e) Introducción del modelo en un computador.
f) Trabajo del modelo como modelo de simulación.

SINERGIA O TOTALIDAD: Indica que los sistemas tienen características propias y una identidad no reducible a las propiedades o características de sus componentes. Este postulado aristotélico de que el todo es más que la suma de las partes refiere

a fenómenos que tienen una identidad que va más allá de sus componentes. Lo importante es la relación. La totalidad apunta a la conservación del todo por la acción recíproca de las partes componentes. Puede señalarse que la sinergia es la propiedad común a todas aquellas cosas que observamos como sistemas. Todo sistema es sinérgico en tanto el examen de sus partes en forma aislada no puede explicar o predecir su comportamiento. La sinergia es, en consecuencia, un fenómeno que surge de las interacciones entre las partes o componentes de un sistema.

SUBSISTEMA: Se entiende por subsistemas a conjuntos de elementos y relaciones que responden a estructuras y funciones especializadas dentro de un sistema mayor. En términos generales, los subsistemas tienen las mismas propiedades que los sistemas y su delimitación es relativa a la posición del observador de sistemas y al modelo que tenga de éstos. Desde este ángulo se puede hablar de subsistemas, sistemas o supersistemas, en tanto éstos posean las características sistémicas.

RETROALIMENTACIÓN: La retroalimentación se define como la propiedad de ajustar la conducta futura a hechos pasados. Esto quiere decir que un sistema, mediante el mecanismo de retroalimentación, regula su comportamiento de acuerdo con su funcionamiento real y no en relación con lo que se espera de él. En otras palabras, se autorregula recogiendo información sobre los efectos de sus decisiones en el entorno. Como el tipo de información es seleccionado, estructural y selectivamente, por los sistemas a través de una codificación, se explica por qué algunos de ellos parecen ignorar señales del entorno que parecen muy evidentes a otros observadores.

Vistas las definiciones anteriores, ahora comenzaremos con Ludwig Von Bertalanffy[113]:

En la parte de tendencias en la teoría de sistemas cabe resaltar las siguientes ideas:

1) En tiempos de cualquier novedad, por trivial que sean es saludada llamándola revolucionaria, está uno harto de aplicar este rótulo a los adelantos científicos.
2) A la zaga de Kuhn, una revolución científica es definida por la aparición de nuevos esquemas conceptuales o «paradigmas».[114]
3) La cibernética es una teoría de los sistemas de control basada en la comunicación (transferencia de información) entre sistema y medio circundante, y dentro del sistema, y en el control (retroalimentación) del funcionamiento del sistema en consideración al medio.[115]

Por lo que hace a Sistemas cerrados y abiertos, tenemos lo siguiente:

[113] Von Bertalanffy, Ludwig, *Teoría General de los Sistemas*, México, FCE, 1986.
[114] *Cfr. Ibidem*. p. 16.
[115] *Cfr. Ibidem*. p. 20.

1) La física ordinaria solo se ocupa de sistemas cerrados, de sistemas que se consideran aislados del medio circundante.
2) En un sistema cerrado, cierta magnitud, la entropía, debe aumentar hasta el máximo, y el proceso acabará por detenerse en un estado de equilibrio.
3) Todo organismo viviente es ante todo un sistema abierto.
4) Por lo que hace a los sistemas abiertos:

> […] Esta teoría ha aclarado muchos fenómenos oscuros en física y biología, y ha conducido asimismo a importantes conclusiones generales, de las cuales sólo mencionaré dos.
>
> La primera es el principio de equifinalidad. En cualquier sistema cerrado, el estado final está inequívocamente determinado por las condiciones iniciales. […] Si se alteran las condiciones iniciales o el proceso, el estado final cambiará también. No ocurre lo mismo en los sistemas abiertos, En ellos puede alcanzarse el mismo estado final partiendo de diferentes condiciones iniciales y por diferentes caminos. Es lo que se llama equifinalidad, y tiene significación para los fenómenos de la regulación biológica.[116]
>
> Otra vía que está vinculada de cerca a la teoría de los sistemas es la moderna teoría de la comunicación. […] La noción general en teoría de la comunicación es la de la información.
>
> Características de la organización, trátese de un organismo vivo o de una sociedad, son nociones como las de totalidad, crecimiento, diferenciación, orden jerárquico, dominancia, control, competencia, etc.[117]
>
> Como ejemplo de la aplicación de la teoría general de los sistemas a la sociedad humana mencionaremos un libro de Boulding intitulado *The Organizational Revolution*. Boulding parte de un modelo de la organización y enuncia las que llama leyes férreas, válidas para cualquier organización. […] Está, asimismo, la ley de las dimensiones óptimas de las organizaciones: mientras más crece una organización, más se alarga el camino para la comunicación, lo cual - y según la naturaleza de la organización- actúa como factor limitante y no permite a la organización crecer más allá de ciertas dimensiones críticas. De acuerdo con la ley de inestabilidad, muchas organizaciones no están en equilibrio estable, sino que exhiben fluctuaciones cíclicas resultantes de la interacción entre subsistemas. […] La importante ley del oligopolio afirma que, si hay organizaciones en competencia, la inestabilidad de sus relaciones, y con ello el peligro de fricción y conflictos aumenta al disminuir el número de dichas organizaciones. Mientras sean relativamente pequeñas y numerosas, salen adelante en una especie de coexistencia, pero si se quedan unas cuantas, o un par, como pasa con los colosales bloques políticos de hoy, los conflictos se hacen devastadores hasta el punto de la mutua destrucción.[118]

[116] *Cfr. Ibidem*. p. 41.
[117] *Ibidem*. p. 47.
[118] *Ibidem*. p. 48.

El sentido de la expresión algo mística «el todo es más que la suma de sus partes» reside sencillamente en que las características constitutivas no son explicables a partir de las características de partes aisladas. […] Sin embargo, si conocemos el total de partes contenidas en un sistema u la relación que hay entre ellas, el comportamiento del sistema es derivable a partir del comportamiento de las partes. [119]

Un sistema puede ser definido como un complejo de elementos interactuantes. Interacción significa que elementos, *p*, están en relaciones, *R*, de suerte que el comportamiento de un elemento *p* es *R* es diferente de su comportamiento en otra relación *R'*. Si los comportamientos en *R* y *R'* no difieren, no hay interacción, y los elementos se comportan independientemente con respecto a las relaciones *R* y *R'*. [120]

En caso de perturbación, el sistema genera fuerzas que contrarrestan dicha perturbación y restauran el estado de equilibrio; son derivaciones del principio del mínimo esfuerzo.[121]

Los teóricos de sistemas coinciden en que el concepto de «sistema» no está limitado a entidades materiales, sino que puede aplicarse a cualquier «todo» que consista en «componentes» que interactúen.[122]

Advertimos de inmediato que se dan sistemas en equilibrio en el organismo, pero que el organismo como tal no puede considerarse como u sistema en equilibrio.

El organismo no es un sistema cerrado sino abierto. Llamamos «cerrado» aun sistema si no entra en él ni sale de él materia; es «abierto» cuando hay importación y exportación de materia.[123]

Un sistema abierto es definido como sistema que intercambia materia con el medio circundante, que exhibe importación y exportación constitución y degradación de sus componentes materiales. [124]

La base del modelo del sistema abierte es la interacción dinámica entre sus componentes, La base del modelo cibernético es el ciclo de retroalimentación, en el cual, por retroalimentación de información, se mantienen un valor deseado (*Sollwert*), se alcanza un blanco, etc. […] La teoría cibernética se basa en retroalimentación e información.[125]

Los sistemas vivos se mantienen en un intercambio más o menos rápido, en degeneración y regeneración, catabolismo y anabolismo de sus componentes. El organismo vivo es un orden jerárquico de sistemas

[119] *Ibidem*. p. 55.
[120] *Ibidem*. p. 56.
[121] *Ibidem*. p. 78.
[122] *Ibidem*. p. 110.
[123] *Ibidem*. p. 125.
[124] *Ibidem*. p. 146.
[125] *Ibidem*. p. 156.

abiertos.[126]

> En lugar de la teoría de los sistemas abiertos, hay otro modelo mejor conocido por la escuela estadounidense. Es el concepto de regulación por retroalimentación, fundamental en cibernética.
>
> Según es generalmente sabido, el modelo básico es un proceso circular en cual parte de la salida es remitida de nuevo, como información sobre el resultado preliminar de la respuesta, a la entrada, haciendo así que el sistema se autorregule, sean en el sentido de mantener determinadas variables o de dirigirse hacia una meta deseada. [127]

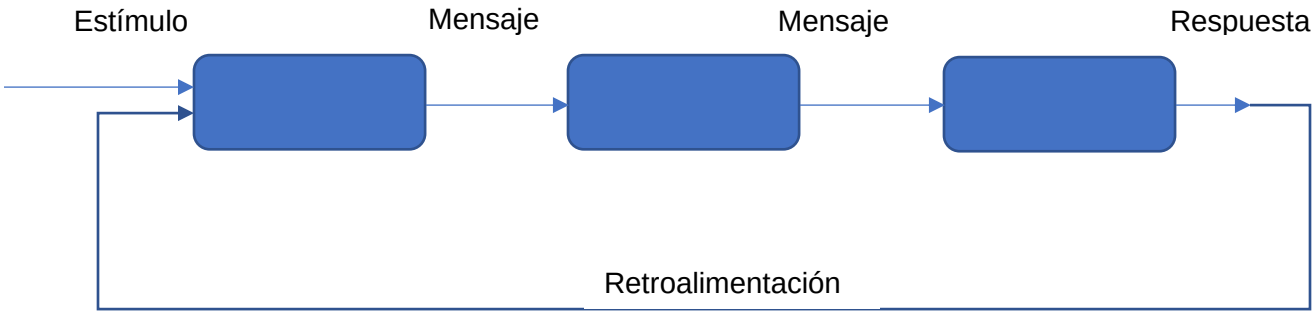


Imagen: Esquema sencillo de retroalimentación.
Tomada de: Von Bertalanffy, Ludwig, Teoría General de los Sistemas, México, FCE, 1986.

Si bien la parte de las teorías de sistemas aparecen en la parte de sistemas cerrados con aplicación en ciencias que hoy se podrían denominar duras; Bertalanffy tiene un apartado de la aplicación de la teoría de sistemas en las ciencias sociales.

> Con fines de discusión entendamos «ciencia social» en sentido amplio, incluyendo sociología, economía, ciencia política, psicología social, antropología cultural, lingüística, buena parte de la historia y las humanidades, etc.
>
> […] en mi opinión puede afirmarse con gran confianza que la *ciencia social es la ciencia de los sistemas sociales*. Por esta razón deberá seguir el enfoque de la ciencia general de los sistemas.[128]

Finalizamos con Bertalanffy con la siguiente idea:

> Todo sistema como entidad investigable por derecho propio debe tener límites, espaciales o dinámicos. Estrictamente hablando, los límites espaciales sólo se dan a la observación ingenua, y todos los límites son en

[126] *Ibidem*. p. 166.
[127] *Ibidem*. p. 167.
[128] *Ibidem*. p. 204.

última instancia dinámicos.[129]

> En contraste con el animal, que tienen un «ambiente» (*Umwelt*) determinado por su organización, el propio hombre crea su mundo, lo que llamamos cultura humana. Entre los requisitos para su evolución están dos factores estrechamente ligados, el lenguaje y la formación de conceptos.[130]

El siguiente autor por tratar es Luhmann. Uno de los discípulos en habla hispana y traductor de su obra, Javier Torres, en su libro Introducción a la Teoría de Sistemas de Niklas Luhmann aborda lo siguiente:

> Para Luhmann, la sociedad es un sistema. Pero, en realidad, ¿Qué es un sistema? […] para la sociología de Luhmann un sistema es sólo una distinción que empleamos en la comunicación: una distinción social. La sociedad no es una estructura petrificada, sino una operación de distinción que se propicia en la comunicación y mediante la cual los seres humanos orientan sus acciones. Un sistema es sólo una forma, por consiguiente, una distinción, una separación, una diferencia. Se opera una distinción trazando una marca que separa dos partes, que vuelve imposible el paso de una parte a la otra sin atravesar la marca. La forma es, pues, una línea de frontera que marca una diferencia y obliga a clarificar qué parte se indica cuando se dice que se encuentra en una parte y dónde se debe comenzar si se quiere proceder a nuevas operaciones.[131]

En su libro sistemas sociales, Luhmann indica que el concepto de teoría de siestas es un concepto unificador de significados y de análisis diversos que llevan a un cierto tipo de revolución científica en términos de Kuhn. Estos análisis se plantean desde tres niveles de cómo repercute el llamado cambio de paradigma en la aplicación de la teoría de sistemas a la teoría general de los sistemas sociales, tal como se aprecia en el siguiente cuadro: [132]

---

[129] *Ibidem*. p. 225.
[130] *Ibidem*. p. 268.
[131] Torres Nafarrete (*sic*), Javier, *Introducción a la Teoría de Sistemas de Niklas Luhmann*, [en línea] México, UNAM, Colección Aprender a Aprender, Serie Perspectivas en la Teoría de Sistemas, 1999, *http://computo.ceiich.unam.mx/webceiich/docs/libro/Introduccion_a_la_teoria_de_sistemas_de_Niklas_Luhmann.pdf* pp. 13-15.
[132] Luhmann, Niklas, *Sistemas sociales, Lineamientos para una teoría general*, México, Universidad Iberoamericana, 2da ed, 1998, p. 27.

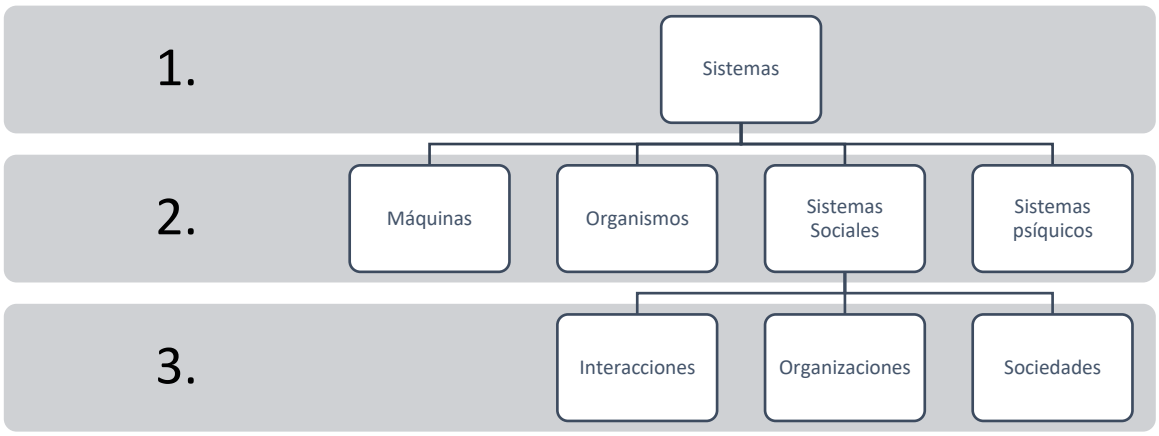


Imagen: Teoría general de los sistemas sociales.
Tomada de: Luhmann, Niklas, Sistemas sociales, Lineamientos para una teoría general, p. 27.

Las ideas relacionadas con la presente investigación son las siguientes:

> El punto de partida de cualquier análisis teórico-sistémico debe consistir en la *diferencia entre sistema y entorno*. […] Los sistemas están estructuralmente orientados al entorno, y sin él, no podrían existir: por lo tanto, no se trata de un contacto ocasional ni tampoco de una mera adaptación. Los sistemas se constituyen y se mantienen mediante la creación y la conservación de la diferencia con el entorno, y utilizan sus límites para regular dicha diferencia. Sin diferencia con respecto al entorno no habría autorreferencia ya que la diferencia es la premisa para la función de todas las operaciones autorreferenciales. En este sentido, *la conservación de los límites (boundary manitenancé)* es la conservación del sistema.[133]
>
> El entorno no es ningún sistema. Para cada sistema el entorno es distinto, ya que cada sistema guarda referencia con su propio entorno. Por lo mismo, el entorno no tiene capacidad de autorreflexión y mucho menos capacidad de acción […] Todo eso no quiere decir, sin embargo, que el entorno dependa del sistema, o que el sistema pueda disponer a placer del entorno. Más bien, lo que se quiere afirmar es que la complejidad, tanto del sistema como del entorno, excluye cualquier forma totalizante de dependencia en uno o en otro sentido.[134]
>
> Los sistemas no son simplemente relaciones (en plural) entre elementos. En alguna parte tiene que estar reglamentada la conexión de las relaciones. Esta reglamentación adopta la forma básica del condicionamiento. Esto significa que una determinada relación entre los elementos se realizará bajo la condición de que eso otro venga o no al caso. […] en este sentido, las relaciones entre los elementos se pueden condicionar mutuamente: algo puede suceder si ocurre lo otro.[135]

[133] *Ibidem*. p. 40.
[134] *Ibidem*. p. 41.
[135] *Ibidem*. p. 46.

Los sistemas tienen límites. Esto es lo que hace diferente al concepto de sistema del de estructura.

Los límites no pueden ser pensados sin un «detrás» y presuponen, por lo tanto, la realidad de un más allá y la posibilidad de rebasarla. Por eso, desde una intelección generé (*sic*) desempeñan una doble función de separación y unificación entre sistema y entorno. Esta doble función se aclara por medio de la distinción entre elemento y relación, y con ello se la remite a la temática de la complejidad. Cuando los límites están definidos con exactitud, los elementos deben atribuirse al sistema o al entorno. Las relaciones, en cambio, pueden acontecer entre sistema y entorno. Por lo tanto, un límite separa elementos, pero no necesariamente relaciones; separa acontecimientos, pero deja fluir efectos causales.[136]

Los sistemas complejos no sólo necesitan adaptarse a su entorno, sino también a su propia complejidad. Tienen que afrontar improbabilidades e insuficiencias internas, y desarrollar disposiciones construidas expresamente para reducir conductas divergentes; sólo así es posible la existencia de estructuras dominantes. Los sistemas complejos, por lo tanto, están constreñidos a la adaptación propia y la adaptación a su propia complejidad. Sólo así es explicable que los sistemas ni puedan seguir sin interrupción los cambios realizados en el entorno, sino que tengan que tomar en cuenta también otros aspectos de la adaptación que finalmente encuentran su razón de ser en la autoadaptación.[137]

A la autorreferencia se le ha concedido una creciente atención a partir de la más reciente investigación de sistemas; se le encuentra, también bajo los títulos de autoorganización y autopoiesis.[138]

El concepto de autorreferencia designa la unidad constitutiva del sistema consigo mismo: unidad de elementos, de procesos, de sistema. «Consigo mismo» quiere decir independiente del ángulo de observación de otros. El concepto no solo define, sino que también incluye una afirmación de un estado de cosas, ya que sostiene que la unidad sólo puede llevarse a cabo mediante una operación relacionante. En consecuencia, la unidad tiene que efectuarse, y no está dada de antemano como individuo, como sustancia o como idea de la propia operación.[139]

Sobre la base de relaciones autorreferenciales de sistemas se puede encauzar una inmensa extensión de los límites de la adaptabilidad estructural y del alcance correspondiente de la comunicación interna del sistema. La mejor manera de comprender esta extensión es partir del concepto de *información*. Una información se da siempre y cuando un acontecimiento selectivo (Externo o interno) pueda accionar selectivamente en el sistema, es decir, cuando pueda seleccionar estados de sistema. Ello presupone la capacidad de orientarse por

[136] *Ibidem*. p. 51.
[137] *Ibidem*. p. 54.
[138] *Ídem*.
[139] *Ibidem*. p. 55.

> diferencias (en forma simultánea o consecutiva) que parece estar atada a su vez a un *modus* operativo autorreferencial del sistema. «Un poco de información» dice Bateson « se puede definir como la diferencia que hace una diferencia». Ello significa que las diferencia empiezan a accionar *como tales* cuando en cuanto pueden ser tratadas como información en los sistemas autorreferenciales.[140]

Del estudio de estos dos pensadores, nos permite tener diferentes elementos para intentar entender nuestra legislación.

Las leyes de transparencia, acceso a la información; protección de datos personales en posesión de sujetos obligados; y de archivos; se encuentran en la categoría y rango de leyes generales.

Actualmente tenemos diferentes leyes generales de carácter administrativo. Leyes Generales en materia ambiental, transparencia, anticorrupción, seguridad, estadística, salud, educación, turismo; etc.

Ahora bien, qué tienen en común las leyes generales, se podría decir que las siguientes:

- Pueden incidir válidamente en todos los órdenes jurídicos parciales que integran al Estado Mexicano.[141]
- Son aquellas respecto de las cuales el Constituyente o el Poder Revisor de la Constitución ha renunciado expresamente a su potestad distribuidora de atribuciones entre las entidades políticas que integran el Estado mexicano, lo cual se traduce en una excepción al principio establecido por el artículo 124 constitucional.
- Estas leyes no son emitidas *motu proprio* por el Congreso de la Unión, sino que se originan en cláusulas constitucionales que constriñen al Congreso a dictarlas y que una vez promulgadas y publicadas, por disposición constitucional, deberán ser aplicadas por las autoridades federales, locales, del Distrito Federal y municipales.
- Por su naturaleza, las leyes generales previstas en la Constitución no se encuentran en la misma situación que las leyes federales y que, por ende, son jerárquicamente superiores a éstas y a las leyes locales, debe tomarse en cuenta que el Pleno de este Alto Tribunal ha reconocido que la validez de las leyes locales sí se encuentra sujeta a lo previsto en una ley general e incluso que, si aquéllas no se apegan a lo previsto en este tipo de leyes, resultarán inconstitucionales.
- El objeto de una ley-general puede consistir en la regulación de un **sistema nacional** de servicios, como sucede con la educación y la salubridad general,

[140] *Ibidem*. p. 61.
[141] Registro digital: 21402 AMPARO EN REVISIÓN 120/2002.
https://sjf2.scjn.gob.mx/detalle/ejecutoria/21402

o establecer un sistema nacional de planeación, como acontece en el caso de los asentamientos humanos.[142]

- Tienen como objeto también, la distribución de competencias en materias concurrentes, por lo que en este caso las leyes locales deben sujetarse a aquellas leyes, pues si bien es cierto que una misma materia queda a cargo de la Federación, Estados y Municipios, también lo es que el Poder Legislativo Federal es quien tiene la facultad de establecer en qué términos participará cada una de estas entidades.

Vale la pena adicionar el contenido de las siguientes tesis cuyos rubros son:

1. Ley general para prevenir y sancionar los delitos en materia de secuestro. Es aplicable tanto para los ilícitos cometidos en el ámbito local como los del fuero federal.
2. Leyes generales. Interpretación del artículo 133 constitucional.
3. Leyes locales en materias concurrentes. En ellas se pueden aumentar las prohibiciones o los deberes impuestos por las leyes generales.

No obstante a lo anterior, también se deben hacer algunas acotaciones respecto a esta premisa:

1) Existen leyes generales en carácter mercantil que no establecen sistemas como la Ley General de Sociedades Cooperativas, Ley General de Sociedades Mercantiles, la Ley General de Títulos y Operaciones de Crédito, Ley General de Organizaciones y Actividades Auxiliares del Crédito.
2) No todas las leyes generales de carácter administrativo establecen sistemas nacionales, como es el caso de la Ley General de Bienes Nacionales que no establece un sistema nacional, pero si menciona un Sistema de Administración Inmobiliaria Federal y Paraestatal y del Sistema de Información Inmobiliaria Federal y Paraestatal, o la Ley General para el Control del Tabaco.
3) Existen Leyes que establecen un sistema nacional sin ser una ley general; como es el caso de la Ley del Sistema Nacional de Información Estadística y Geográfica; Ley Nacional del Sistema Integral de Justicia Penal para Adolescentes.
4) En la conformación de un Sistema Nacional pueden estar vinculadas diferentes leyes generales o leyes no generales.
    a. Leyes Generales en Material Ambiental.
    b. Leyes con carácter no general como en el caso de Anticorrupción.

Las leyes generales para ser debidamente aplicadas se pueden agrupar por

[142] Registro digital: 7570 Asunto: CONTROVERSIA CONSTITUCIONAL 29/2000. *https://sjf2.scjn.gob.mx/detalle/ejecutoria/7570*

materias como se aprecia en el siguiente esquema:

- Ambiental
  - Cambio climático
  - Desarrollo Forestal Sustentable
  - Equilibrio Ecológico y Protección al Ambiente
  - Prevención y Gestión Integral de los Residuos
  - Vida silvestre
- Cultura
  - Cultura y Derechos Culturales
  - Cultura Física y Deporte (Que también podría entrar en Educación por su autoridad central)
  - Bibliotecas
- Salud
  - Salud
  - Control de Tabaco
  - Atención y Protección a Personas con la Condición del Espectro Autista
  - Detección Oportuna del Cáncer en la Infancia y la Adolescencia
  - Inclusión de las Personas con Discapacidad
- Electoral
  - Instituciones y procedimientos electorales
  - Partidos Políticos
  - Medios de Impugnación en materia electoral
  - Delitos Electorales
- Seguridad
  - Seguridad Pública
  - Víctimas
  - Materia de Desaparición Forzada de Personas, Desaparición Cometida por Particulares y del Sistema Nacional de Búsqueda de Personas
  - Prevención Social de la Violencia y la Delincuencia
  - Prevenir, Investigar y Sancionar la Tortura y Otros Tratos o Penas Crueles, Inhumanos o Degradantes
  - Prevenir y Sancionar los Delitos en Materia de Secuestro
- Anticorrupción
  - Anticorrupción
  - Contabilidad Gubernamental
  - Responsabilidades Administrativas
  - Fiscalización y Rendición de Cuentas
  - En materia penal, administrativo e institucionales
    - Código Penal
    - Orgánica de la Administración Pública Federal
    - Fiscalía General de la República

        - Tribunal Federal de Justicia Administrativa
- Transparencia, Acceso a la Información y Datos Personales
    - Archivos
    - Datos Personales
        - Sujetos Obligados
        - En Posesión de Particulares
    - Transparencia y Acceso a la Información Pública
        - Rendición de Cuentas

El sistema de Transparencia (para abreviar) es un sistema (valga la redundancia) que tiene una autorreferencia o íntima relación con otros dos sistemas. Por un parte el de Anticorrupción al ser parte del Sistema Nacional Anticorrupción; y por otra parte, con el sistema de Estadística, los cuales se enlazan por medio del Sistema Nacional de Transparencia. De este modo podríamos llamar a este subsistema como Sistema Nacional de Transparencia y Anticorrupción (SNTA) tal como se aprecia en el siguiente cuadro:

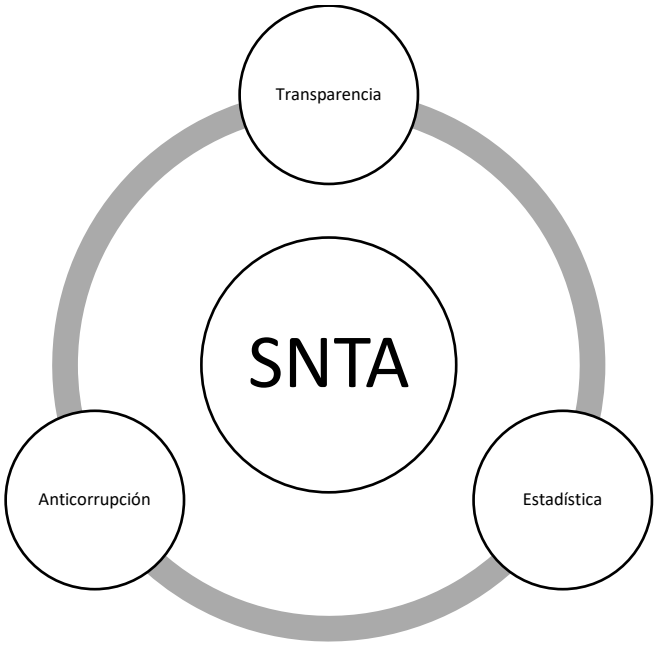


Imagen: Sistema Nacional de Transparencia y Anticorrupción.
Fuente: Elaboración propia.

Ahora bien, el Sistema Nacional de Transparencia cuenta a su vez con 5 componentes como se muestra a continuación:

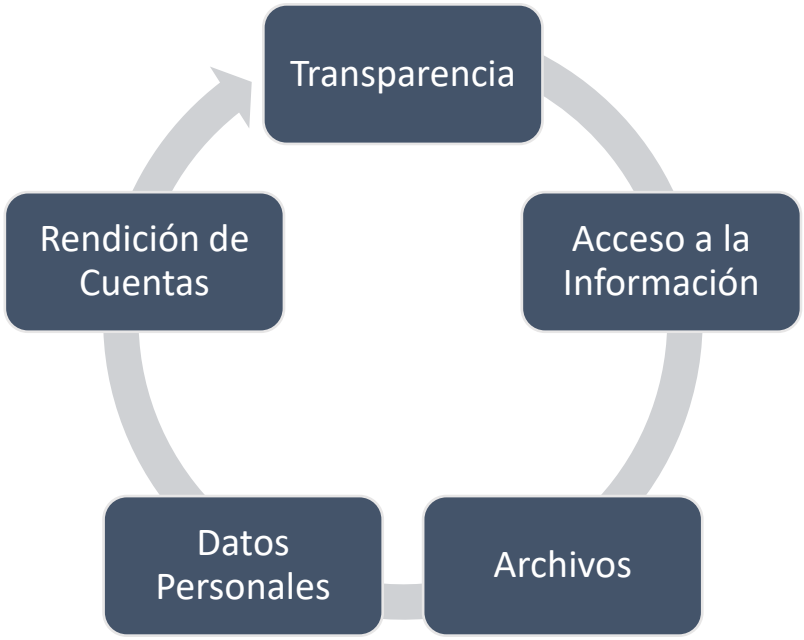


Imagen: Componentes del Sistema Nacional de Transparencia.
Fuente: Elaboración propia.

Cabe destacar que el componente de Rendición de Cuentas se comparte con el de anticorrupción por medio de la ley de fiscalización y rendición de cuentas.

Por último, de manera esquemática, el sistema de transparencia quedó comprendido de la siguiente forma:

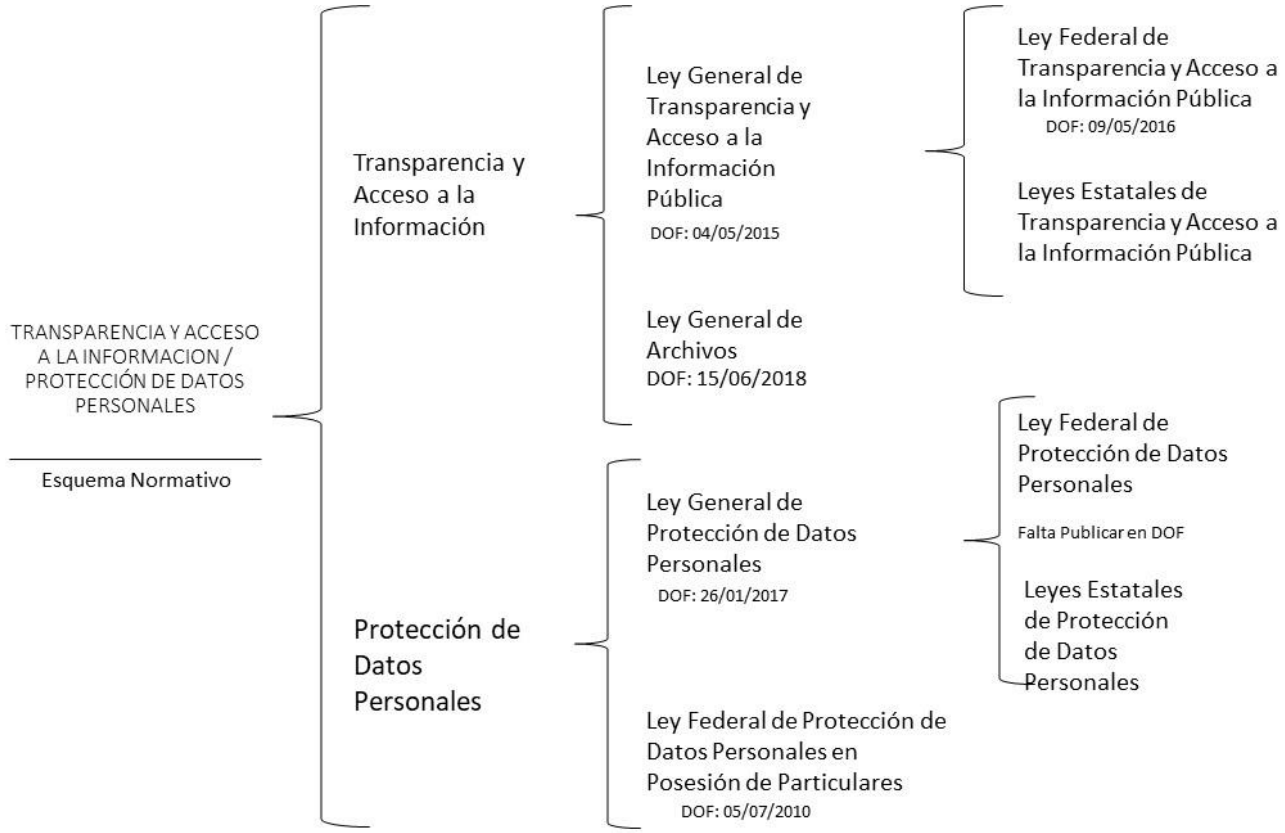


Imagen: Esquema normativo de transparencia, acceso a la información y protección de datos personales.
Fuente: Elaboración propia.

Capítulo 2. Aspectos del Big Data

2.1. Datos, tipos de Datos y Metadatos

En este mundo global, con contenidos 24/7 los 365 días del año, con procesadores que alcanzan velocidades alucinantes y con capacidades de almacenamiento cada vez más grandes y diferenciadas (disco duro/nube); donde cualquier persona puede encontrar información y datos de todo tipo, forma, tamaño; donde cualquier persona escribe y se expresa de todo tipo de temas; donde el problema ya no es dónde encontrarla; sino la calidad de la información; creo que bien se puede decir que estamos en presencia de una nueva revolución "industrial" o tal vez una sub-revolución.

Por si fuera poco, hablar del tamaño de la información también es difícil de comprender el volumen que llegamos a tener; de manera cotidiana hablamos de toneladas de información, y en cuanto al volumen a lo más que llegamos a conversar en tamaño de Terabytes; y eso, porque cuando llegamos a comprar un ordenador, el vendedor nos llega a comentar que existen computadores con capacidad de almacenamiento de 1 terabyte. Tan solo al momento de escribir esta tesis, acabo de comprar un disco duro externo de 4 Teras, y ya llevo la mitad del almacenamiento.

Sin embargo, a escalas macro, hablar de "teras" es como decir *bytes*, así de abismal es lo que ocurre en la actualidad. Procesar una gran cantidad de datos de todos lados del mundo requiere sistemas y "discos" con una capacidad inconmensurable de almacenamiento. Alguna vez llegué a leer por ahí que la edición dominical del *The New York Times* incluyendo todos sus suplementos era el equivalente a un mes o más de información que la procesada en la edad media en toda Europa.

Para Verónica López Sabater, "el dato se ha convertido en insumo fundamental de cualquier proceso económico. En su estado bruto -sin tratar, aislado-, el dato carece a priori de valor. Es de su tratamiento, procesamiento y análisis científico de donde se extrae conocimiento útil y original".[143]

Así que hoy se puede decir que estamos en una nueva era de la economía que, de acuerdo con Sabater, estaríamos en presencia de la cuarta era industrial, para lo cual se utilizará el siguiente cuadro:[144]

Era Industrial	Elemento Característico
Primera	Sustentada en innovaciones tecnológicas como la máquina de vapor

[143] López Sabater, Verónica, (coord.) *Economía de los Datos, Riqueza 4.0*, España, Ariel, 2017, p. 7.
[144] Basado en *Ibidem*, p. 11.

Era Industrial	Elemento Característico
Segunda	Electricidad y el petróleo como detonantes
Tercera	Eclosionó gracias al desarrollo de las tecnologías de la información y la comunicación (TIC)
Cuarta	Los Datos: Un elemento más etéreo. Economía del conocimiento.

Los datos están catalogados en una nueva economía que favorece nuevos modelos de negocio, donde el uso y desarrollo de las plataformas digitales darán paso a la llamada economía de red, la cual, a su vez, implicaría nuevas regulaciones, así como oportunidades laborales.

La demanda de perfiles digitales no solo ha crecido de forma exponencial en los últimos años, sino que está llamada a ejercer un papel relevante en la nueva estructura del mercado de trabajo. Principalmente, destacan estas tres figuras: el director de datos o *chief data officer* (CDO), el ingeniero de datos o *big data engineer* y los directores de seguridad y protección de datos. Los rasgos que se deben destacar de este tipo de perfiles laborales son el dominio de múltiples disciplinas (matemática, estadística, ingeniería, informática y negocios) y la adaptación a entornos cambiantes.[145]

Según Manuel Castells, estamos en la era que él denomina sociedad red, la cual es una nueva estructura social dominante en la llamada era de la información, cuya característica principal no es la acumulación de conocimiento e información, sino la aplicación de ambos en la construcción del aparato de conocimiento y procesamiento de la "información/comunicación en un círculo de retroalimentación acumulativo entre la innovación y sus usos"[146]

En la era de la información, la tendencia visible es la globalización total de la economía; pero advierte Castells que un mercado mundial completamente abierto no será en un futuro inmediato.

> Las organizaciones y empresas exitosas son aquellas capaces de generar conocimientos y procesar la información; de adaptarse a la variable geométrica de la economía global; de tener flexibilidad para reconvertir sus fines y medios de manera rápida; y de innovar «cuando la innovación se convierte en el ara clave de la competencia». La «empresa red» «materializa la cultura de la economía informacional/global: transforma señales en bienes mediante el procesamiento del conocimiento».[147]

[145] *Ibidem*, p. 14.
[146] Castells, Manuel, citado por Aldana Rendón, Mario, "Reseña de" *Castells: la era de la información. Realizades y reflexiones sobre la globalización*, [en línea], México, Espiral, vol. VI, no. 18, 2000, Redalyc, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.redalyc.org/articulo.oa?id=13861811* p.286.
[147] *Ibidem*, p. 290.

Castells propone una hipótesis con respecto a que la sociedad informacional está constituyéndose en torno a flujos: "de capital, de información, de tecnología, de imágenes, sonidos, y símbolos; flujos que no son un elemento más de la organización social, sino la expresión de los procesos que dominan nuestra vida económica, política y simbólica"[148]

En 2015, el Instituto para el Futuro (IFTF por sus siglas en inglés) realizó un estudio donde se analizaron cinco aspectos que podrían ser claves en el desarrollo del tratamiento de datos, de la privacidad, de la transformación digital y de la omnicanalidad. Dicho estudio obtuvo las siguientes conclusiones:

1. La economía de la información. Lo más seguro es que se acabe regularizando el mercado de la información. La venta, donación e intercambio de información útil y estandarizada en mercados abiertos será una realidad pronto.
2. Ecosistemas conectados. Espacios conscientes, conectados y con capacidad de reacción. El Internet de las Cosas parece destinado a ser otra fuerza democratizadora.
3. Toma de decisiones aumentada. La ayuda e importancia de la inteligencia artificial en los procesos de toma de decisiones llegará a unos puntos elevados de forma inimaginable.
4. Comunicación multisensorial. La información ya no se distribuye por los canales tradicionales. Los seres humanos no somos menos, terminaremos absorbiendo la información a través de nuestros múltiples sentidos.
5. Tecnología pro-preservación de la privacidad. La justicia en el campo de la privacidad se conseguirá, según el estudio, aprovechando la oleada de herramientas dirigidas al usuario destinadas a tal efecto. El problema está ahí, y ya es tangible para la mayoría de los usuarios.[149]

Hoy en día es prácticamente un hecho que vivimos en un mundo con una sobrecarga de información, donde el reto es buscar cómo manejar ese enorme cúmulo de datos; todavía es de considerarse que tanto organizaciones públicas como privadas aun no conocen la forma de extraer todo el valor que pueda proporcionarles nuestra huella digital.

En 2020 más de 7.000 millones de personas tendrán un mínimo de 30.000 millones de dispositivos. Todos estos dispositivos habrán creado 44 zettabytes de datos (o 44 billones de gigabytes), según Gartner e IDC respectivamente. Sin embargo, a pesar de que las empresas saben que pueden obtener valor de esta información, las expectativas que se reflejan en este estudio desvelan cierta desorientación en las empresas:

[148] *Ibidem*, p. 293.
[149] BBVA, *La era de la información: cinco claves de su futuro*, [en línea] España, BBVA, secc. Innovación, 11 de agosto de 2017, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.bbva.com/es/informacion-cinco-claves-futuro/*

1) El 49% de las empresas no sabe cómo convertir todos sus datos en información útil.
2) El 70% afirma que puede extraer conocimiento de los datos, pero tan solo el 30% está siempre conectado y puede actuar basándose en esa información en tiempo real.
3) El 52% reconoce que no utiliza sus datos de manera eficaz o que se encuentran desbordados por una sobrecarga de información.
4) Solo el 24% se considera "muy bueno" a la hora de convertir los datos en conocimiento e información útil para su negocio.[150]

Entonces, en este mundo lleno de datos e información por todas partes, hay que recordar que un dato, para Davenport y Prusak es una "representación simbólica (numérica, alfabética, algorítmica, etc.) de un atributo o variable cuantitativa o cualitativa. Los datos describen hechos empíricos, sucesos y entidades. Los datos son la mínima unidad, son elementos primarios de información que por sí solos son irrelevantes y no suelen decir nada sobre el porqué de las cosas. Un dato es un número de teléfono, un apellido, una hora, la coordenada de un lugar."[151]

Se podría decir que, en el camino del conocimiento, los datos son como una madeja que hasta que se va desarrollando hasta obtener conocimiento.[152]

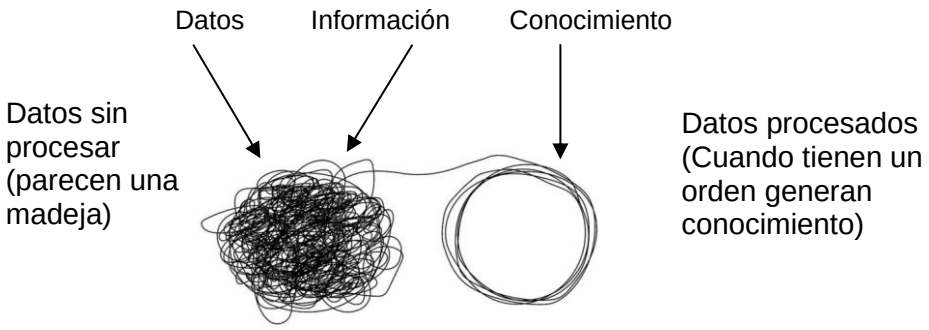


Imagen: Camino al conocimiento.
Basada en: Tascón Mario, Coullaut Arantza, *Big Data y el Internet de las cosas, Qué hay detrás y cómo nos va a cambiar*, España, Catarata, 2016, p. 9.

Ahora bien, para que los datos se conviertan en información, éstos deberán tener un valor que pueda añadírseles mediante diferentes formas:
1) Cálculo: Los datos pueden procesarse matemática o estadísticamente.
2) Categorización: Conocer las unidades de medida para interpretar los datos.

[150] BBVA, *Una de cada dos empresas reconoce que no sabe obtener valor de los datos*, España, BBVA on line, secc. Big Data, 18 de agosto de 2017, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.bbva.com/es/dos-empresas-reconoce-sabe-obtener-valor-datos/*
[151] Citados por Tascón Mario, Coullaut Arantza, *Big Data y el Internet de las cosas, Qué hay detrás y cómo nos va a cambiar*, España, Catarata, 2016, p. 9.
[152] Basados en *Ídem*.

3) Condensación: Saber resumir los datos (agregación).
4) Contextualización: Aportaciones a los contextos y el propósito con el que se generaron.
5) Corrección: Eliminar los errores e inconsistencias de los datos.[153]

Por su parte, Wolfran distingue diferentes tipos de categorías:[154]

a) Datos estructurados: Almacenables en filas y columnas.
b) Datos Semiestructurados: Los que no se ajustan a un esquema fijo y explicito, documentos xml, los blogs o los sensores.
c) Datos No Estructurados: Los que se presentan en un formato que no puede ser fácilmente indexado en tablas relacionales para el análisis; como los datos de las imágenes, audio, video o los de las redes sociales.

Para la empresa IBM, la clasificación de datos en *big data* es la siguiente:[155]

1. Datos de Internet y Redes Sociales. Datos de Blogs, Wikis, otras plataformas de internet y diferentes redes sociales.
2. Datos máquina a máquina. Tecnologías de conectividad entre dispositivos.
3. *Big Transaction Data*. Registros de facturación o los registros detallados de las llamadas (CDR, *Call Detail Record*) que contienen información sobre su origen, destino y duración.
4. Biométricos. Información concerniente al cuerpo humano como retina, reconocimiento facial, huellas dactilares, etc.
5. Generados por humanos. Datos que dejan una huella digital; es decir al "rastro" que dejan los usuarios al usar el internet o las redes sociales; los cuales configuran la identidad en la Red.

El otro tema a considerar en este punto es el de los metadatos. La Asamblea General de las Naciones Unidas en su acuerdo A/C.3/71/L.39 de fecha 31 de octubre de 2016 relacionado con el septuagésimo primer periodo de sesiones, relativo al tema el derecho a la privacidad en la era digital, menciona que "si bien los metadatos pueden aportar beneficios, algunos tipos de metadatos, tomados en conjunto, pueden revelar información personal y pueden dar indicación del comportamiento, las relaciones sociales, las preferencias privadas y la identidad de una persona"[156]

La misma Asamblea General de las Naciones Unidas en su acuerdo A/HRC/23/40 de fecha 17 de abril de 2013 relacionado con el vigésimo tercer periodo de sesiones, relativo al Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, menciona que: "El carácter dinámico de la tecnología no solo ha cambiado la forma en que puede llevarse a cabo la vigilancia,

[153]Tomados de *Ibidem*. p. 10.
[154] Tomados de *Ibidem*. p. 11.
[155] Tomados de *Ibidem*. p. 11.
[156] ONU, *El derecho a la privacidad en la era digital*, A/C.3/71/L.39 de fecha 31 de octubre de 2016, [en línea] Asamblea General - UN Digital Library, 2016, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://digitallibrary.un.org › A_C-3_71_L-39-ES* p. 3.

sino también "qué" puede vigilarse. Al facilitar la creación de oportunidades de comunicación e intercambio de información, Internet también ha posibilitado la elaboración de un gran volumen de datos de transacciones de personas y acerca de estas. Esta información, conocida como datos de las comunicaciones o metadatos, incluye información personal sobre particulares, su ubicación y actividades en línea, así como registros e información conexa sobre los correos electrónicos y los mensajes que envían o reciben."[157]

Como se puede advertir, el concepto y uso de metadatos es tan importante como para que lo aborde la misma Asamblea de Naciones Unidas. Senso y de la Rosa Piñeiro, consideran que dicho término fue acuñado por Jack Myers en la década de los 60's del siglo pasado para describir conjunto de datos. "La primera acepción que se le dio (y actualmente la más extendida) fue la de dato sobre dato, ya que proporcionaban la información mínima necesaria para identificar un recurso. En este mismo trabajo se afirma que *puede incluir información descriptiva sobre el contexto, calidad y condición o características del dato*."[158] Para estos autores redefinen el concepto de metadato como: "toda aquella información descriptiva sobre el contexto, calidad, condición o características de un recurso, dato u objeto que tiene la finalidad de facilitar su recuperación, autentificación, evaluación, preservación o interoperatividad."[159]

Por su parte, para el Archivo General de la Nación, en su "Breviario de Metadatos", se menciona que los metadatos son: "información estructurada, creada digitalmente, capturada, administrada y preservada, con independencia del soporte del recurso o recursos a los que describen. La estructura reside en la sintaxis y los vocabularios, expresados mediante modelos abstractos, y se realiza en las normas, esquemas y perfiles de aplicación de metadatos."[160]

En el caso de la UNAM, tenemos el documento denominado Lineamientos para la Integración de Repositorios Universitarios en el Repositorio Institucional de la UNAM, publicados en la Gaceta UNAM de fecha 19 de octubre de 2020, donde se definen a los metadatos en el lineamiento 5° (quinto), fracción XIII como:

> 5. Para efectos de los presentes Lineamientos se entenderá por: […]
> XIII. Metadatos. Datos estructurados y actualizados que describen el contexto y las características de contenido, captura, procesamiento,

[157] ONU, *Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión*, acuerdo A/HRC/23/40 de fecha 17 de abril de 2013 [en línea] Asamblea General - UN Digital Library, 2013, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://undocs.org/es/A/HRC/23/40* p. 5.

[158] Senso, José A. y de la rosa Piñeiro, Antonio, *El concepto de metadato. Algo más que descripción de recursos electrónicos*, [en línea] Brasil, Revista Scielo, v. 32, n. 2, may-ago 2003, [fecha de consulta: 3 de diciembre de 2022] Disponible en:
https://www.scielo.br/j/ci/a/ZHtZZfYnJfKqVn4tGNSw4yv/?format=pdf&lang=es p. 97.

[159] *Ibidem*, p. 99.

[160] AGN, *Breviario de metadatos*, [en línea] México, AGN, Serie: Temas fundamentales de preservación digital, no. 4, 2016, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.gob.mx/cms/uploads/attachment/file/228991/InterPARES_4_020617.pdf* p. 25.

calidad, condición, acceso y distribución de un conjunto de datos, que sirven para facilitar su búsqueda, identificación y uso.[161]

La importancia o ventajas de los metadatos de acuerdo con Senso y de la Rosa Piñeiro son las siguientes:[162]

1) Incrementan la Accesibilidad: Los metadatos hacen posible la búsqueda de información en múltiples colecciones a la vez, por medio del mapeo de sistemas heterogéneos de búsqueda los cuales permiten consultar en diferentes bases de datos con una sola ecuación de búsqueda.
2) Disminución del tráfico en la Red: Esto se logra por medio de indexaciones (hacer índices) que permiten hacer representaciones del objeto de búsqueda, lo que disminuye el ancho de banda para hacer búsquedas.
3) Expandir el uso de la información: Facilitan la versión de versiones digitales de un único objeto.
4) Control de versiones: Atiende al ciclo de vida del metadato, así como a las modificaciones realizadas en el transcurso del tiempo. Las versiones pueden incluso ser compartidas en con diferentes tipos de públicos.
5) Aspectos Legales: Están relacionados con restricciones en la explotación de contenidos, informar sobre derechos de autor, control sobre información de tipo restringida, licencias de uso e interoperabilidad.
6) Preservación del objeto original: Tiene que ver con la protección o cuidado de los contenidos digitales.

Ahora bien, por lo que hace a la tipología de los metadatos, Anne Gilliland propone diferentes categorías y funciones de metadatos tal como se muestra en el siguiente cuadro:[163]

Tipo	Definición	Ejemplos
Administrativo	Metadatos usados en la gestión y administración de recursos de información	Adquisición de información Control de derechos y reproducciones Documentación de requisitos legales Información sobre localización Criterios de selección para la

[161] UNAM, *Lineamientos para la Integración de Repositorios Universitarios en el Repositorio Institucional de la UNAM,* [en línea] México, en "Gaceta UNAM" Número 5,156, 19 de octubre de 2020, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.gaceta.unam.mx/wp-content/uploads/2020/10/201019.pdf* p. 36.
[162] *Cfr*. Senso, José A. y de la rosa Piñeiro, Antonio, *op. cit*. p. 100.
[163] Gilliland-Swetland, Anne, *La definición de los metadatos*, en Getty Trust, J. Paul Coord. "Introducción a los Metadatos. Vías a la información digital", [en línea] USA, 1999, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *http://d2aohiyo3d3idm.cloudfront.net/publications/virtuallibrary/0892365358.pdf* pp. 3-4.

Tipo	Definición	Ejemplos
		digitalización control de las distintas versiones
Descriptivo	Metadatos usados para descubrir o identificar información sobre recursos	Catalogación de registros Ayudas para la búsqueda Índices especializados Relaciones hiperenlazadas entre recursos Anotaciones de usuarios
Conservación	Metadatos relacionados con la conservación de recursos de información	Documentación de recursos sobre la condición física Documentación de acciones tomadas para conservar versiones físicas y digitales de los recursos, ej. Regeneración y migración de datos
Técnico	Metadatos relacionados con el funcionamiento de los sistemas o el comportamiento de los metadatos	Documentación de hardware o software Digitalización de la información ej, formatos, ratios de compresión, ajustes Control de tiempo de respuesta de los sistemas Autenticación y seguridad de los datos, ej. claves cifradas, contraseñas
Uso	Metadatos relacionados con el nivel y el tipo de uso de los recursos de información	Registro de exhibiciones Seguimiento de usos y de usuarios Uso repetido de contenido e información sobre versiones múltiples

Asimismo, además de los distintos tipos de metadatos y de sus diversas funciones, existen varias características asociadas con los mismos. Algunos de los atributos clave de los metadatos se muestran en la siguiente tabla:[164]

Atributo	Características	Ejemplos
Fuente de los metadatos	Metadatos internos generados para un objeto informático en el momento de su creación o digitalización	Nombres de los registros e información sobre la etiqueta inicial Estructuras de Directorio Formato del registro y

[164] *Ibidem*. p. 4.

Atributo	Características	Ejemplos
	Metadatos externos relacionados con un objeto informático creados posteriormente, generalmente por alguien distinto del agente original	esquema de comprensión Fichas de registro y de catalogación Derechos y otra información legal
Métodos para la creación de metadatos	Metadatos automáticos generados por ordenador Metadatos manuales creados por individuos	Índices de palabras clave Registros de las operaciones de los usuarios Copias descriptivas tales como registros de catalogación y metadatos *Dublín Core*
Carácter de los metadatos	Metadatos creados por individuos que no son ni especialistas temáticos ni en información, generalmente el creador original del objeto informático Metadatos expertos creados por especialistas temáticos o en información, generalmente no se trata del creador original	Metadatos creados para una página Web personal Sistemas personales de archivo Encabezamientos temáticos especializados Registros MARC Ayudas para la búsqueda en archivos
Estatus	Metadatos estadísticos que no cambian una vez creados Metadatos dinámicos que pueden cambiar con el uso o con la manipulación de un objeto informático Metadatos de larga duración para asegurar que el objeto siga siendo accesible y se pueda usar Metadatos de corta duración. Principalmente de tipo operacional	Título, Procedencia y fecha de creación de un recurso de información Estructura de directorio Registros de las operaciones de los usuarios Resolución de imágenes Formatos Técnicos y procesamiento de información Información sobre derechos Conservación y administración de la documentación

Atributo	Características	Ejemplos
Estructura	Metadatos estructurados que responden a una estructura previsible, tanto si esta es estándar como si no lo es Metadatos no estructurados que no responden a una estructura previsible	MARC TEI Y EAD Formatos de bancos de catos locales Campos de notas y anotaciones sin estructurar
Semántica	Metadatos controlados que responden a un vocabulario estándar o a un formulario de autoridad Metadatos no controlados que no responden ni a un vocabulario estándar no a un formulario de autoridad´	AAT ULAN AACR2 TGN Notas de texto libre Metaetiquetas HTML
Nivel	Metadatos de colección relacionados con colecciones de objetos informáticos Metadatos relacionados con objetos informáticos individuales, a menudo incluidos dentro de una colección	Registro a nivel de colección, p. ej. Registro MARC o ayuda para la búsqueda Índices especializados Transcripción de fechas y de texto a pie de imagen Información sobre el formulario

Concuerdo con la opinión de Anil Hirwade cuando manifiesta que “Los metadatos son una parte clave de la infraestructura de información necesaria para ayudar a crear orden en el caos de la Web, infundiendo descripción, clasificación y organización para ayudar a crear más útiles almacenes de información.”[165]

Dado que hoy en día la gestión y administración de los documentos y de la información misma se ha vuelto automatizada, se ha vuelto necesario la generación de una serie de normativas de carácter técnico y de aplicación legal con el fin de

[165] Hirwade, Anil y Hirwade Mangala, “*Metadata Harvesting Service in India*”, [en línea], EUA, en Library Herald, 2006, vol. 44, n. 4, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *http://eprints.rclis.org/9295/* p. 5.

regular la estructura, composición e interoperabilidad de los metadatos.
A continuación, se mencionarán diferentes normas de carácter técnico más conocido relacionadas con el manejo de los metadatos.

A) DUBLIN CORE

La Iniciativa de Metadatos *Dublin Core*™, o "DCMI", es una organización que apoya la innovación en el diseño de metadatos y las mejores prácticas en la ecología de los metadatos. DCMI funciona abiertamente y está respaldado por un modelo de membresía de paga.

La Iniciativa de Metadatos *Dublin Core*™ (DCMI) apoya la innovación compartida en el diseño de metadatos y las mejores prácticas en una amplia gama de propósitos y modelos comerciales.

DCMI hace esto de la siguiente manera:

- Gestionar la conservación a largo plazo y el desarrollo de espacios de nombres de términos de metadatos y especificaciones ;
- Realización de una conferencia internacional anual ;
- Curación y disponibilidad abierta de los activos de la reunión, incluidos los procedimientos, los informes del proyecto y las actas de la reunión;
- Creación y entrega de recursos de capacitación en las mejores prácticas de metadatos, incluidos tutoriales, seminarios web y talleres; y
- Coordinar la comunidad global de voluntarios de DCMI .[166]

En su DCMI *Metadata Terms*, se describe que:

> Este documento es una especificación autorizada y actualizada de todos los términos de metadatos mantenidos por *Dublin Core™ Metadata Initiative*. Se incluyen los quince términos del conjunto de elementos de metadatos *Dublin Core*™ (también conocido como "*Dublin Core*") más varias docenas de propiedades, clases, tipos de datos y esquemas de codificación de vocabulario. El "*Dublin Core*" más estos vocabularios de extensión se denominan colectivamente "términos de metadatos DCMI" ("términos *Dublin Core*" para abreviar). Estos términos están destinados a ser utilizados en combinación con términos de metadatos de otros vocabularios compatibles en el contexto de los perfiles de aplicación.
> Los términos de metadatos de DCMI se expresan en vocabularios RDF para su uso en datos vinculados. Los creadores de metadatos no RDF pueden usar los términos en contextos como XML, JSON, UML o bases de datos relacionales sin tener en cuenta tanto el identificador global como las implicaciones formales de los aspectos específicos de RDF de las definiciones de términos. Dichos usuarios pueden tomar las relaciones de dominio, rango, subpropiedad y subclase como sugerencias de uso y centrarse en el texto en lenguaje natural de definiciones, notas de uso y ejemplos.[167]

[166] Dublin Core, *About DCMI, s/d,* [en línea] [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.dublincore.org/about/*
[167] Dublin Core, *DCMI Metadata Terms*, 2020, [fecha de consulta: 3 de diciembre de 2022] Disponible

Según el Instituto de Investigaciones de la Amazonia Peruana (IIAP) el total de 15 elementos que integran el formato *Dublin Core*™, se pueden clasificar en tres grupos, que indican la clase o el ámbito de la información que contienen:[168]

Elementos relacionados principalmente con el contenido del recurso	Elementos relacionados principalmente con el recurso cuando es visto como una propiedad intelectual	Elementos relacionados principalmente con la temporalidad y formato del documento, así como su identificación
Título Tema o Palabras Clave Descripción Fuente Lenguaje Relación Cobertura	Autor o Creador Editor otras colaboraciones o colaboradores Derechos	Fecha Tipo de recurso Formato Identificador del recurso

Esta norma se ha correlacionado con la ISO 15836:2009[169] así como con la Norma ANSI/NISO z39.85-2007

B) METADATOS DE GESTIÓN DOCUMENTAL[170]

Electronic Recordkeeping Metadata Standard (Nueva Zelanda 2008)	Aborda los metadatos en el punto de captura y los metadatos de procesos de gestión archivística para identificar y describir el contenido, el contexto y la estructura de los documentos de archivo, las condiciones de su uso y seguridad, las relaciones con otros documentos de archivo, personas y negocios que son objeto de transacción, y para identificar eventos pasados y futuros que documentan las

en: *http://dublincore.org/specifications/dublin-core/dcmi-terms/2020-01-20/*

[168] Citado por Dirección General de Repositorios Universitarios, *Estándar de Datos de Objetos Digitales Dublin Core Cualificados (DC)*, [en línea] México, UNAM, octubre 2019, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://dgru.unam.mx/wp-content/uploads/2019/10/D.ST_.DGRU_CDI_009_2015_C_OD_Dublin_Core.pdf* p. 1.

[169] La norma tiene una actualización a 2011. Esta norma internacional establece una norma para la descripción de recursos de información de distintos dominios informativos, conocido conjunto de elementos de metadatos *Dublin Core*. Como en la RFC 3986, esta norma internacional no limita cómo debe de ser un recurso. Esta norma internacional define los elementos típicamente utilizados en el contexto de un perfil que limita o especifica su uso de acuerdo con los requisitos y políticas locales o basadas en la comunidad. Sin embargo, no define detalles de implementación, que está fuera del campo de aplicación de esta norma.

[170] Tr. Barnard, Alicia, *et. al*. *Breviario de Metadatos*, [en línea], México, AGN, Serie: Temas fundamentales de preservación digital, 2016, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.gob.mx/cms/uploads/attachment/file/228991/InterPARES_4_020617.pdf* pp. 54- 65.

	acciones de gestión archivística que afectan a la autenticidad y la integridad.
Recordkeeping Metadata Standard (Australia, 2008)	Está basada en un modelo multientidad, que permite la descripción de cinco entidades separadas: documento de archivo, agente, actividad, mandato y relación. Describe los metadatos mínimos necesarios para asegurar que los documentos de archivo siguen siendo accesibles y utilizables a lo largo del tiempo.
ISO 23081-1:2006 *Information and Documentation–Records Management Processes–Metadata for Record–* parte 1[171]	Cubre los principios que regulan los documentos de archivo y sus metadatos, los procesos que les afectan, los sistemas en los que son creados y mantenidos, y las organizaciones responsables de su administración.
ISO 23081-2:2009 *Information and Documentation–Records Management Processes–Metadata for Records–* parte 2: marco conceptual	Identifica las cuestiones que surgen en la implantación de metadatos para administrar documentos de archivo y las opciones para abordar estas cuestiones.
ISO/TR 23081-3:2011 *Information and Documentation–Records Management Processes–Metadata for Records–* parte 3: método de autoponderación	Proporciona recomendaciones para ejecutar una autoponderación para identificar el estado actual de captura y administración de metadatos, identificar prioridades y requisitos clave, evaluar el progreso en el desarrollo de un marco ver metadatos, y evaluar la disponibilidad del sistema y el proyecto para incluir funcionalidades de metadatos en un sistema.
Treasury Board of Canada Standard on Metadata	Establece recomendaciones para aplicar metadatos de gestión archivística a recursos de información con valor de negocio para el Gobierno de Canadá, utilizando el conjunto genérico de elementos de metadatos ISO 23,081.
Registros de metadatos en la Organización de las Naciones Unidas: Archives and Records Management Section (ARMS)	El documento detalla la importancia de los metadatos normalizados de gestión archivística para asegurar el registro de una adecuada información contextual acerca de transacciones, ayudar en la recuperación de los documentos de archivo, controlar el acceso, facilitar la transparencia, reducir el uso fraudulento y el acceso no autorizado, promover en la eficacia y la economía, y proporcionar una cota para medir la

[171] Esta ISO tiene una actualización en 2017:ISO 23081-1

	calidad y dar soporte a la auditoría.

C) METADATOS ARCHIVÍSTICOS[172]

DACS *(Describing Archives: a Content Standard)*	Es una norma multinivel uno "conjunto de reglas neutrales con respecto a la salida" aplicable a todos los soportes.
EAD *(Encoded Archival Description)*	Proporciona una codificación en XML para descripciones archivísticas. adopta una aproximación multinivel a la descripción, proporcionando información acerca de una colección como un todo y luego descomponiéndola en grupos, series y (si fuese significativo) en ítems individuales.
METS *(Metadata Encoding and Transmission Standard)*	Es una especificación decodificación y transmisión de datos para comportar los metadatos necesarios tanto para la administración de objetos digitales dentro de un depósito como para el intercambio de tales objetos entre depósitos. Una función clave de esta norma es estructurar o empaquetar otros metadatos o datos para su intercambio o suministro. puede anidar o vincularse a otros metadatos basados en XML. Un cierto número o tipo de archivos de computadora pueden describirse o vincularse con un registro METS, haciendo posible representar recursos digitales muy complejos (como todo un libro digitalizado, con datos bibliográficos, imágenes y texto transcrito).

D) METADATOS PARA BIBLIOTECAS (NORMAS DE CATALOGACIÓN)[173]

MARC 21	Son normas de transmisión de metadatos utilizadas por las bibliotecas para la representación y la comunicación de información bibliográfica y relacionada con la forma legible por máquina. Esta norma fue resultado de la combinación y la revisión de los formatos MARC De Estados Unidos y Canadá para hacerlos más accesibles internacionalmente.
RDA *(Resource Description and Access)*	Proporciona recomendaciones instrucciones sobre la descripción de y el acceso a recursos para todos los tipos de contenidos y soportes.

[172] Basado en Barnard, Alicia, *et. al*. *Breviario de Metadatos*, *op. cit.* pp. 59-60.
[173] Basado en *Ibidem*. p. 61-63.

AARC2 *(Anglo-American Cataloguing Rules)*	Proporciona recomendaciones sobre la catalogación de recursos digitales, y da soporte para la agrupación de registros bibliográficos para mostrar las relaciones entre las obras y sus creadores. Este es un producto de suscripción, integrado basado en navegador y en línea que incluye instrucciones, flujos de tareas, concordancias de esta norma con diferentes esquemas y otros recursos relacionados
MODS *(Metadata Object Description Schema)*	Como esquema XML, Puede utilizarse para. Aportar datos seleccionados de registros MARC XXI ya existente, así como para crear registros originales descriptivos de recursos. puede utilizarse para poner metadatos para su recogida, representar la descripción del recurso original en síntesis XML, y ofrece un conjunto de elementos qué es más rico que *Dublin Core*, compatible con datos bibliotecarios, y más sencillo que el formato MARC completo.
OAI-PMH *(Open Archives Initiative-Protocol for Metadata Harvesting)*	Es una importante iniciativa para facilitar la interoperabilidad de registros de metadatos. proporciona un medio automatizado para solicitar registros de metadatos de depósitos conformes con OAI, y para agregar los metadatos para que se puedan usar desde un solo lugar. los proveedores de datos forman sus conjuntos de metadatos disponibles para su recopilación utilizando *Dublin Core* sencillo en un formato normalizado XML.
PREMIS	Proporciona un diccionario de datos de elementos de metadatos centrales orientados a dar soporte a la preservación digital. Específicamente, el diccionario de datos define los metadatos de preservación que dan soporte a la viabilidad, representabilidad, comprensibilidad, autenticidad e identidad de los objetos digitales en un contexto de preservación. enfatizan los “metadatos implantables”: rigurosamente definidos, soportados por recomendaciones para su producción, administración y uso, y orientados hacia flujos de tareas automatizados; e incorpora neutralidad técnica: no se hacen asunciones acerca de tecnologías, estrategias, almacenamiento de metadatos y administración, etcétera, de la preservación.
7 SEPIADES *(SEPIA Data Element Set)*	Es un conjunto de elementos de datos multinivel para catalogar colecciones fotográficas, recomendado por

	la *European Commission on Preservation and Access*. La descripción jerárquica la determina el usuario, que puede crear tantos niveles y sus niveles cómo se requieran, desde el nivel de Instituto o depósito hasta descender al nivel de un solo ítem.

2.1.1 Normatividad europea en metadatos

Ahora bien, por lo que hace a la normatividad de carácter jurídico se mencionan las siguientes:

En la Unión Europea, se ha publicado diferente normativa referente a los metadatos; para efectos de esta investigación no se abordarán las legislaciones de cada país europeo; solo se tomarán las normas comunitarias:

Directiva 2003/98/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público[174]

Esta norma reconoce:

(2) La evolución hacia la sociedad de la información y del conocimiento afecta a la vida de todos los ciudadanos de la Comunidad, en particular al permitirles contar con nuevos medios para acceder y adquirir el conocimiento.

(3) Los contenidos digitales desempeñan un papel importante en esta evolución. La producción de contenidos ha dado lugar durante los últimos años, y sigue haciéndolo actualmente, a un fenómeno de rápida creación de empleo. La mayor parte de estos puestos de trabajo los crean pequeñas empresas emergentes.

(4) El sector público recoge, produce, reproduce y difunde una amplia gama de información relativa a numerosos ámbitos, por ejemplo, información social, económica, geográfica, meteorológica o turística y sobre empresas, patentes y educación.

De acuerdo con el artículo 1. El objeto de la directiva es establecer un "conjunto mínimo de normas que regulen la reutilización y los instrumentos prácticos que faciliten la reutilización de los documentos existentes conservados por organismos del sector público de los Estados miembros."

[174] Parlamento Europeo, *Directiva 2003/98/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público,* [en línea] s/d., [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32003L0098*

No obstante, lo anterior, esta Directiva tenía una serie de puntos que quedaban excluidas de ella y que de acuerdo con su artículo 2 (dos) son:

> 2. La presente Directiva no se aplicará a:
> a) los documentos cuyo suministro sea una actividad que se salga del ámbito de la misión de servicio público de los organismos del sector público afectados, definida con arreglo a la legislación o a otras normas de obligado cumplimiento del Estado miembro o, en su ausencia, definida en consonancia con la práctica administrativa común del Estado miembro de que se trate;
> b) los documentos sobre los que existan derechos de propiedad intelectual por parte de terceros;
> c) los documentos a los que no pueda accederse en virtud de regímenes de acceso de los Estados miembros, por motivos, entre otros, de:
> - protección de la seguridad nacional (esto es, seguridad del Estado), defensa o seguridad pública,
> - confidencialidad estadística o comercial;
> d) los documentos conservados por las entidades de radiodifusión de servicio público y sus filiales, y por otras entidades o sus filiales para el cumplimiento de una misión de radiodifusión de servicio público;
> e) los documentos conservados por instituciones educativas y de investigación, tales como centros escolares, universidades, archivos, bibliotecas y centros de investigación, con inclusión, si procede, de organizaciones creadas para la transferencia de los resultados de la investigación;
> f) los documentos conservados por instituciones culturales tales como museos, bibliotecas, archivos, orquestas, óperas, ballets y teatros.

Ante esto, es que se emitió la Directiva 2007/2/CE y más recientemente la Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo de 20 de junio de 2019 la cual es la norma vigente.

DIRECTIVA 2007/2/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 14 de marzo de 2007 por la que se establece una infraestructura de información espacial en la Comunidad Europea (Inspire)[175]

Esta Directiva reconoce a la Directiva 2003/98/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público como objetivos complementarios a los de la presente Directiva.

Esta Directiva debía aplicarse a los datos espaciales detentados por las autoridades públicas o en nombre de ellas, así como a la utilización de tales datos por parte de dichas autoridades en el ejercicio de sus funciones públicas. Sin embargo, bajo ciertas condiciones, debe aplicarse también a la información espacial en poder de personas físicas o jurídicas diferentes de las autoridades públicas, siempre que tales personas así lo soliciten.

[175] Parlamento Europeo, *DIRECTIVA 2007/2/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 14 de marzo de 2007 por la que se establece una infraestructura de información espacial en la Comunidad Europea (Inspire),* [en línea] s/d., [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32007L0002*

Dentro de las definiciones, resaltan las siguientes:

> Artículo 3. A efectos de la presente Directiva se entenderá por:
>
> 1) «infraestructura de información espacial»: metadatos, conjuntos de datos espaciales y los servicios de datos espaciales; los servicios y tecnologías de red; los acuerdos sobre puesta en común, acceso y utilización; y los mecanismos, procesos y procedimientos de coordinación y seguimiento establecidos, gestionados o puestos a disposición de conformidad con lo dispuesto en la presente Directiva;
>
> 2) «datos espaciales»: cualquier dato que, de forma directa o indirecta, hagan referencia a una localización o zona geográfica específica;
>
> 3) «conjunto de datos espaciales»: una recopilación identificable de datos espaciales;
>
> 4) «servicios de datos espaciales»: las operaciones que puedan efectuarse, a través de una aplicación informática, sobre los datos espaciales contenidos en dichos conjuntos de datos o en los metadatos correspondientes;
>
> 5) «objeto espacial»: la representación abstracta de un fenómeno real que corresponde a una localización o zona geográfica específica;
>
> 6) «metadatos»: la información que describe los conjuntos y servicios de datos espaciales y que hace posible localizarlos, inventariarlos y utilizarlos;
>
> 7) «interoperabilidad»: la posibilidad de combinación de los conjuntos de datos espaciales y de interacción de los servicios, sin intervención manual repetitiva, de forma que el resultado sea coherente y se aumente el valor añadido de los conjuntos y servicios de datos;

Reglamento (CE) 1205/2008 de la Comisión, de 3 de diciembre de 2008, por el que se ejecuta la Directiva 2007/2/CE del Parlamento Europeo y del Consejo en lo que se refiere a los Metadatos[176]

Este Reglamento reconoce que es necesaria la definición de un conjunto de elementos de metadatos que permitan identificar y clasificar el recurso de información para el que se haya creado el metadato, y determinar su localización geográfica y su referencia temporal, así como la calidad y validez de los metadatos, la conformidad con las normas de aplicación sobre la interoperabilidad de los servicios y conjuntos de datos espaciales, las restricciones de acceso y uso, y la

[176] Parlamento Europeo, *Reglamento (CE) 1205/2008 de la Comisión, de 3 de diciembre de 2008, por el que se ejecuta la Directiva 2007/2/CE del Parlamento Europeo y del Consejo en lo que se refiere a los Metadatos,* [en línea] s/d., [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ%3AL%3A2008%3A326%3A0012%3A0030%3AES%3APDF*

organización responsable del recurso.

El objeto de este Reglamento de acuerdo con el artículo 1° es: El presente Reglamento establece los requisitos para la creación y el mantenimiento de metadatos para conjuntos de datos espaciales, series de conjuntos de datos espaciales y servicios de datos espaciales correspondientes a los temas indicados en los anexos I, II y III de la Directiva 2007/2/CE.

DIRECTIVA (UE) 2019/1024 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 20 de junio de 2019 relativa a los datos abiertos y la reutilización de la información del sector público[177]

Esta Directiva reconoce que La Directiva 2003/98/CE del Parlamento Europeo y del Consejo ha sido modificada de forma sustancial. Dado que deben hacerse nuevas modificaciones y en aras de la claridad, conviene proceder a la refundición de dicha Directiva.

Asimismo, reconoce que:

> Desde la adopción del primer conjunto de normas sobre reutilización de la información del sector público, el volumen de datos, incluidos los públicos, ha aumentado exponencialmente en todo el mundo, al tiempo que se están generando y recopilando nuevos tipos de datos. Paralelamente, se está produciendo una constante evolución de las tecnologías para el análisis, la explotación y el tratamiento de datos, como el aprendizaje automático, la inteligencia artificial y el internet de las cosas. Esa rápida evolución tecnológica permite la creación de nuevos servicios y aplicaciones basados en el uso, la agregación o la combinación de datos. Las normas originales de 2003, y modificadas en 2013 están desfasadas con respecto a estos rápidos cambios y, como consecuencia de ello, pueden perderse las oportunidades económicas y sociales que ofrece la reutilización de los datos públicos.

El objeto de esta Directiva es: fomentar el uso de datos abiertos y estimular la innovación de los productos y servicios, la presente Directiva establece un conjunto de normas mínimas que regula la reutilización y los dispositivos prácticos destinados a facilitar la reutilización de:

> a) los documentos existentes conservados por organismos del sector público de los Estados miembros;
> b) los documentos existentes conservados por empresas públicas […]
> c) los datos de investigación […]

Dentro de las definiciones que se podrían considerar más importantes son:

[177] Parlamento Europeo, *DIRECTIVA (UE) 2019/1024 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 20 de junio de 2019 relativa a los datos abiertos y la reutilización de la información del sector público,* [en línea] s/d., [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=uriserv:OJ.L_.2019.172.01.0056.01.SPA*

Artículo 2 Definiciones: A efectos de la presente Directiva , se entenderá por: […]

7) «anonimización»: proceso por el que se transforman documentos en documentos anónimos que no se refiere a una persona física identificada o identificable o al proceso de convertir datos personales que se hayan anonimizado, de forma que el interesado no sea identificable o haya dejado de serlo;

8) «datos dinámicos»: documentos en formato digital, sujetos a actualizaciones frecuentes o en tiempo real, debido, en particular, a su volatilidad o rápida obsolescencia; los datos generados por los sensores suelen considerarse datos dinámicos;

9) «datos de investigación»: documentos en formato digital, distintos de las publicaciones científicas, recopilados o elaborados en el transcurso de actividades de investigación científica y utilizados como prueba en el proceso de investigación, o comúnmente aceptados en la comunidad investigadora como necesarios para validar las conclusiones y los resultados de la investigación;

10) «conjuntos de datos de alto valor»: documentos cuya reutilización está asociada a considerables beneficios para la sociedad, el medio ambiente y la economía, en particular debido a su idoneidad para la creación de servicios de valor añadido, aplicaciones y puestos de trabajo nuevos, dignos y de calidad, y del número de beneficiarios potenciales de los servicios de valor añadido y aplicaciones basados en tales conjuntos de datos;

2.1.2 Normatividad en México en materia de metadatos

En cuanto a la legislación nacional se abordarán diferentes disposiciones a continuación:

Ley del Sistema Nacional de Información Estadística y Geográfica

Esta Ley tiene dos artículos que refieren a los metadatos:

Sección V. De las Unidades del Estado

ARTÍCULO 33.- Las Unidades del Estado distintas al Instituto, cuando desarrollen actividades relacionadas con la producción, integración, conservación y difusión de Información de Interés Nacional, deberán: […]

VI. Resguardar y conservar la Información, así como los metadatos o especificaciones concretas de la aplicación de las metodologías que hubieren utilizado en la elaboración de la misma, en la forma y términos que, previo acuerdo con el coordinador de la Unidad que corresponda, señale el Instituto.

> ARTÍCULO 88.- El Instituto deberá definir las metodologías que habrán de utilizarse en la realización de las Actividades Estadísticas y Geográficas, a través de Internet, antes de su implantación, a fin de recibir y, en su caso, atender las observaciones que se formulen al efecto.
> De igual forma, el Instituto deberá dar a conocer y conservar los metadatos o especificaciones concretas de la aplicación de las metodologías que se hubieren utilizado en la elaboración de la Información. […]

Dado que el INEGI es parte del Sistema Nacional de Información Estadística y Geográfica, se emitieron dos normas relativas al manejo de metadatos con fines geográficos.

Norma Técnica para la elaboración de Metadatos Geográficos

Esta norma fue publicada en el Diario Oficial de la Federación el 24 de diciembre de 2010 y tiene por "objeto establecer las disposiciones mínimas para la elaboración de metadatos de los grupos de datos geográficos de interés nacional o que sirvan para generar estos, realizados por las Unidades del Estado que integran el Sistema, ya sea por sí mismas o por terceros, así como promover su armonización y homogeneidad."

Dos definiciones relacionadas con metadatos son las siguientes:

> Metadatos.- Los datos estructurados que describen las características de contenido, calidad, condición, acceso y distribución de la información estadística o geográfica.
>
> Perfil de Metadatos.- La selección de elementos de metadatos necesarios para satisfacer los requerimientos de documentación de información en alguna organización o país, estableciendo los tamaños y dominios para cada elemento. Así mismo, debe contener los elementos de metadatos obligatorios de la norma adoptada.

Norma Técnica para la Elaboración de Metadatos para proyectos de generación de Información Estadística Básica y de los componentes estadísticos derivados de proyectos geográficos.

Esta norma fue publicada en el Diario Oficial de la Federación el 03 de septiembre de 2015 y tiene como objeto "establecer las disposiciones mínimas para la elaboración de los metadatos de los proyectos para la generación de información estadística básica de interés nacional y de los componentes estadísticos derivados de proyectos geográficos, que lleven a cabo las Unidades del Estado que integran el Sistema Nacional de Información Estadística y Geográfica (Sistema), con el propósito de promover su armonización y homogeneidad."

Esta norma define Metadatos como "Datos estructurados que describen las características del contenido, captura, procesamiento, calidad, condición, acceso y distribución de la información estadística o geográfica"

Ley General de Transparencia y Acceso a la Información Pública

Esta Ley fue publicada en el Diario Oficial de la Federación el 04 de mayo de 2015, y por lo que hace a los metadatos se tiene lo siguiente:

> Artículo 3. Para los efectos de la presente Ley se entenderá por:
>
> VI. Datos abiertos: Los datos digitales de carácter público que son accesibles en línea que pueden ser usados, reutilizados y redistribuidos por cualquier interesado y que tienen las siguientes características: […]
>
> b) Integrales: Contienen el tema que describen a detalle y con los metadatos necesarios;

Ley General de Archivos

Esta Ley fue publicada en el Diario Oficial de la Federación el 15 de junio de 2018, y por lo que hace a los metadatos se tiene lo siguiente:

> Artículo 4. Para los efectos de esta Ley se entenderá por:
> XLI. Metadatos: Al conjunto de datos que describen el contexto, contenido y estructura de los documentos de archivos y su administración, a través del tiempo, y que sirven para identificarlos, facilitar su búsqueda, administración y control de acceso;
>
> Artículo 43. segundo párrafo […] Los documentos de archivo electrónicos que pertenezcan a series documentales con valor histórico se deberán conservar en sus formatos originales, así como una copia de su representación gráfica o visual, además de todos los metadatos descriptivos.

Acuerdo mediante el cual se aprueban los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales.

Este acuerdo fue publicado en el Diario Oficial de la Federación el 12 de febrero de 2018, y por lo que hace a los metadatos se tiene lo siguiente:

> Definiciones
>
> Artículo 2. Además de las definiciones previstas en el artículo 3 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, para los efectos de los presentes Lineamientos se entenderá por:
>
> IV. Metadatos: Información en un formato estructurado y comúnmente utilizado que describe el contexto, calidad, condición o características de los datos personales;
>
> Metadatos
>
> Artículo 18. El responsable deberá entregar al titular o transmitir al responsable receptor, 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.

Criterios para la formulación de Cláusulas en Contratos que tengan por objeto el tratamiento de Datos Personales[178]

Estos criterios fueron generados por la Auditoría Superior de la Federación en junio de 2021, y tienen como objetivo establecer los criterios a considerar por parte de las unidades administrativas en su calidad de Áreas Requirentes en la suscripción de contratos con personas físicas o morales y que conlleven la obtención o prestación de servicios a través de los cuales se traten datos personales.

En este contexto, este documento especifica en el numeral I.3 Datos Objeto de tratamiento inciso C. fracción II, lo siguiente:

I.3 DATOS OBJETO DE TRATAMIENTO

C. Datos personales objeto de tratamiento

II. Se consideran datos sensibles, los siguientes: Estado de salud presente o futuro; filiación partidista; opiniones políticas, creencias religiosas, filosóficas o morales, particularmente cuando estas puedan dar origen a discriminación o su revelación conlleven un riesgo grave para la persona titular de los datos; afiliación sindical; origen racial; información genética; reconocimiento facial, de iris o huellas digitales sistematizadas y que permitan realizar un tratamiento automatizado de estos, así como la generación de metadatos o perfiles de los titulares; preferencia sexual, entre otros.

Ley Federal de Telecomunicaciones y Radiodifusión

Esta Ley fue publicada en el Diario Oficial de la Federación el 14 de julio de 2014, y si bien no mencionan a los metadatos de manera textual, de la lectura del artículo 190 fracción II, se tiene una obligación para los concesionarios de telecomunicaciones y en su caso autorizados respecto a la conservación de metadatos.

Artículo 190. Los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán:

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:

[178] Auditoría Superior de la Federación, *Criterios para la formulación de cláusulas en contratos que tengan por objeto el tratamiento de datos* personales, [en línea] México, ASF, 2021, [fecha de consulta: 3 de diciembre de 2022] Disponible en: https*://www.asf.gob.mx/uploads/2301_Proteccion_de_Datos/Criterios_para_la_formulacion_de_clausulas_en_contratos.pdf* p. 9.

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.

Estándar de Metadatos para la Interoperabilidad Jurídica de Repositorios Universitarios

Este estándar en su primera edición fue publicado el 01 de julio de 2021 en la Universidad Nacional Autónoma de México indica que “Un estándar de metadatos es un modelo, norma o patrón que permite establecer uniformidad en la descripción de un contenido digital, está formado por un conjunto de elementos diseñados para identificar la información pertinente que deberá incluirse al describir un determinado tipo de contenido digital. A cada elemento se le asignan un nombre, una definición y una etiqueta; se cuida su sintaxis; se describen su obligatoriedad y ocurrencia, utilizando para ello un vocabulario controlado siempre que sea posible.”[179]

Asimismo, se indica que “Un repositorio con interoperabilidad jurídica es el que está dotado de normatividad jurídica (p. ej. políticas, lineamientos y términos de uso) compatible con otros repositorios, y cuyos contenidos digitales cuentan con metadatos que incluyen información suficiente, correcta y actualizada para facilitar a los usuarios de cualquier parte del mundo la identificación de los usos permitidos y el respeto a los derechos de autor y de propiedad industrial.”[180]

[179] UNAM, *Estándar de metadatos para interoperabilidad jurídica de repositorios universitarios*, [en línea], México, UNAM, 2021, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://dgru.unam.mx/wp-content/uploads/2021/08/Est%C3%A1ndar-de-Metadatos-de-Interoperabilidad-Jur%C3%ADdica-_Final.pdf* p. 16.
[180] *Ibidem*, p. 20.

Cada vez es más recurrente el uso de los metadatos para fines comerciales; sin embargo, cabe señalar que, a inicios de 2021, la aplicación de WhatsApp realizó un cambio en sus políticas de privacidad, por medio de las cuales anunciaba algunos tipos de datos que transferiría a sus plataformas hermanas, garantizando por un lado los datos personales como los que se aprecian en el siguiente cuadro:[181]

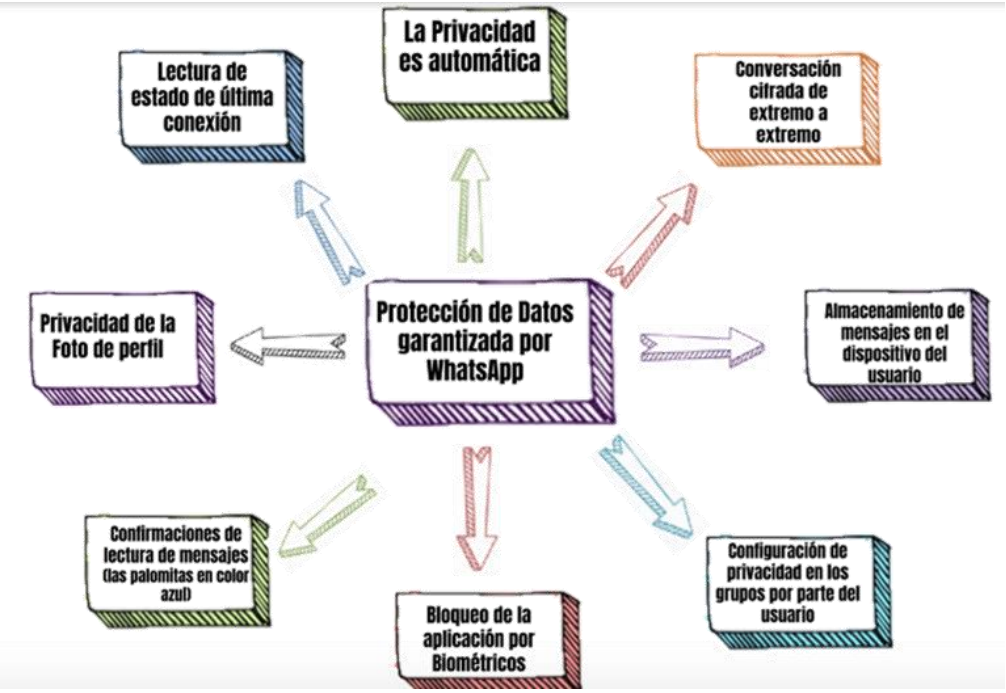


Imagen: Protección de datos garantizada por WhatsApp.
Fuente: Elaboración propia.

Sin embargo, la parte más debatida es la correspondiente con los metadatos de índole comercial, como la hora de conexión, información de localización, si se compra por medio de la aplicación, dispositivo en el que se utiliza la aplicación; entre otros.

Lo anterior, significa que ya no nada más los datos personales se deben proteger; pero ahora hay que cubrir y cuidar también los datos ocultos o mejor dicho, metadatos.

2.2. Características del *Big Data*

Con la nueva forma de entender la economía de los datos, la irrupción de los datos abiertos, los metadatos y en general el desarrollo tecnológico, dentro del marco del denominado Internet de las Cosas, han hecho que en la época actual tengamos datos, información y más información.

[181] Torres Jiménez, Raúl, *WhatsApp, ¿Qué es lo que se vulnera?*, [en línea] México, Revista Consultoría, enero 14 de 2021, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://revistaconsultoria.com.mx/whatsapp-lo-se-vulnera/*

Se sabe que el *big data* nació con las características 3V's: Volumen, Velocidad y Variedad; sin embargo, con el correr de los años estas características se han ido ampliando de tal manera que al día de hoy se dice que son 7V's:

1. Volumen: la cantidad de datos que maneja.
2. Velocidad: tener la infraestructura y los procesos necesarios para tratar los datos de forma ágil y en el menor tiempo posible para aplicar estrategias de cambios.
3. Variedad: tener distintas fuentes de recopilación de datos sobre diferentes aspectos relacionados con el negocio y los consumidores. No solo data estructurada, sino de diferentes tipos: comportamiento, conversaciones, afinidades, fotos, vídeos, etc.
4. Veracidad: cómo de acertada es la data que tenemos. A mayor volumen, mayor es el trabajo para organizar esos datos.
5. Valor: saber cómo tratar la data que se recopila para sacarle un valor a la misma que ayude a tomar decisiones acertadas. (Que también tiene que ver con el valor económico de los datos personales; por ejemplo)
6. Variabilidad: las diferentes interpretaciones que pueden resultar en el proceso.
7. Visión: el poder tener una visión clara de cómo proceder en base (*sic*) a los diferentes patrones e interpretaciones de comportamiento del consumidor.[182]

Y dado que cada vez existen más V's se podrían añadir:

a) Viabilidad. se trata de la capacidad que tienen las organizaciones en generar en un uso eficaz del gran volumen de datos que manejan. Para ello es necesario filtrar a través de la información y seleccionar cuidadosamente los atributos y factores que son capaces de predecir los resultados que más interesan.
b) Visualización de los Datos. Tiene que ver con el modo en que los datos son presentados. una vez que los datos son procesados, se necesitan representar visualmente de manera que sean legibles y accesibles, procurando encontrar patrones y posibles claves ocultas.[183]

También se dice que puede existir una dimensión adicional a las características de los *big data* y es la correspondiente a la complejidad, esto es, que los datos

[182] Bello, Elena, *Big Data: qué es, para qué sirve y por qué es importante*,[en línea] España, IEB SCHOOL, Blog, 15 de octubre de 2021, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.iebschool.com/blog/valor-big-data/*

[183] *Cfr*. Instituto de Ingeniería del Conocimiento, *Las 7 V del Big Data: características más importantes*, [en línea] España, IIC-UAM, Sección Innovación, 2019, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.iic.uam.es/innovacion/big-data-caracteristicas-mas-importantes-7-v/#viabilidad*

“provienen de múltiples fuentes, lo que dificulta la conexión, combinación, limpieza y transformación de datos cruzados. Sin embargo, necesita conectarse y correlacionar relaciones, jerarquías y vínculos”[184]

Existen diferentes tipologías de los *big data*, a continuación, se verán diferentes tipos de ellas.

En cuanto a la tipología de datos por fuente de información Jeffrey Needham indica lo siguiente:[185]

Datos generados por el ser humano (*Human generated*)	Encontramos en particular las plataformas de redes sociales (Facebook, LinkedIn), blogs (*Blogger*, *Wordpress*) y *micro-blogging* (Twitter, *Tumblr*), noticias sociales (*Digg*, *Reddit*), marcadores sociales (Yahoo, Amazon).
Datos generados por la máquina (*Machine generated*)	Se producen a partir de fuentes como GPS, IoT, sensores RFID, estaciones de monitoreo de eventos meteorológicos, instrumentos científicos, mercados financieros, sistemas de comercio de alta frecuencia, dispositivos biomédicos, entre otros
Datos generados por los negocios (*Business generated*)	Son todos los datos, creados por personas o máquinas, que se generan internamente en una empresa que registra todas las actividades basadas en datos de los procesos empresariales. Muchos de ellos son datos históricos almacenados estáticamente en bases de datos relacionales y representan pagos, pedidos, producción, inventario, ventas y datos financieros.

Por su parte Sunil Soares propone lo siguiente:[186]

[184] Calderón Berra, Santiago Michele, “Un zoom a los big data”, *Revista Reporte*, [en línea] México, Núm. 110-2017, Septiembre 2017, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://app.vlex.com/#WW/vid/850330511* p. 17.
[185] Citado por Calderón Berra, *op. cit.* p. 19.
[186] Soares, Sunil, Not Your Type? Big Data Matchmaker On Five Data Types You Need To Explore Today, Dataversity, EUA, 03 de junio de 2012., *http://www.dataversity.net/not-your-type-big-data-matchmaker-on-five-data-types-you-need-to-explore-today/#*

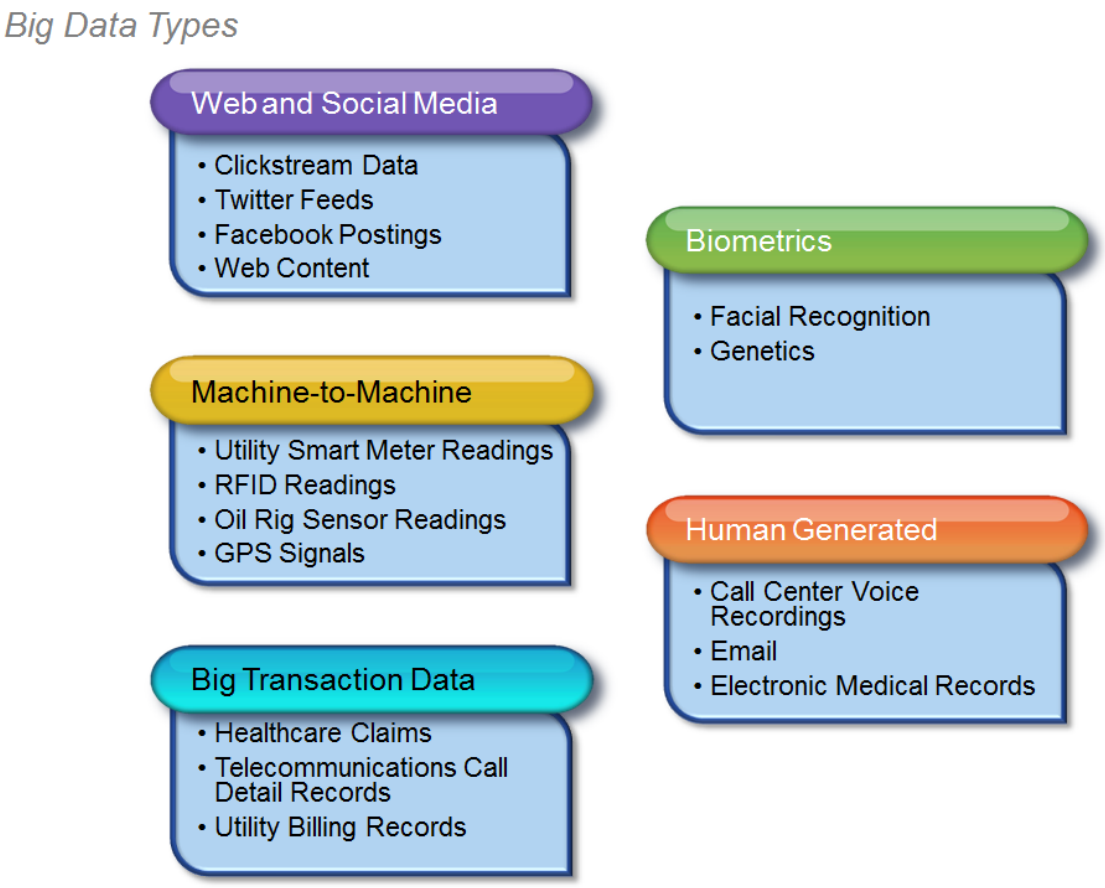


Imagen: Tipos de Big Data.
Tomada de: Soares, Sunil, *¿Not Your Type? Big Data Matchmaker On Five Data Types You Need To Explore Today*, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.dataversity.net/not-your-type-big-data-matchmaker-on-five-data-types-you-need-to-explore-today/#*

1. Web y redes sociales

Esto incluye el flujo de clics y los datos de las redes sociales como Facebook, Twitter, LinkedIn y blogs. Los programas de gobernanza de *big data* serán cada vez más necesarios para integrar estos datos con los datos maestros y con los procesos comerciales centrales, como los programas de fidelización de clientes. El programa de gobernanza de *big data* debe establecer políticas con respecto al uso aceptable de los datos de las redes sociales, especialmente debido a que las regulaciones y los precedentes evolucionan continuamente. El programa también necesita establecer pautas con respecto al uso aceptable de cookies, especialmente cookies de terceros, para rastrear a los usuarios y personalizar sus interacciones en la web. Los metadatos también son fundamentales para la web y las redes sociales. Por ejemplo, dos sitios pueden medir el término "visitantes únicos" de manera diferente para el análisis del flujo de clics.

2. Datos de máquina a máquina

Máquina a máquina (M2M) se refiere a tecnologías que permiten que los sistemas inalámbricos y alámbricos se comuniquen con otros dispositivos. M2M utiliza un dispositivo como un sensor o medidor para capturar un evento (como velocidad, temperatura, presión, flujo o salinidad) que se transmite a través de una red inalámbrica, cableada o híbrida a una aplicación que traduce el evento capturado en significativo. información. Las comunicaciones M2M crean el llamado "Internet de las cosas". El programa de gobernanza de big data debe establecer una serie de políticas en torno a los datos M2M. Por ejemplo, el programa debe elaborar pautas sobre el uso aceptable de la geolocalización y los datos RFID que se pueden utilizar para crear un perfil de las personas y potencialmente violar su privacidad. El programa también necesita establecer políticas de retención en torno a los enormes volúmenes de datos M2M que pueden abrumar fácilmente los presupuestos de TI si no se controlan adecuadamente. El programa de gobernanza de big data también debe abordar cualquier problema de calidad de los datos, como las tasas de lectura de RFID en entornos con alto contenido de humedad y mucha congestión.

3. Datos de grandes transacciones

Esto incluye reclamos de atención médica, registros de detalles de llamadas de telecomunicaciones y registros de facturación de servicios públicos. Los datos de grandes transacciones están cada vez más disponibles en formatos semiestructurados y no estructurados. Los desafíos del gobierno de la información, como los metadatos, la calidad de los datos, la privacidad y la gestión del ciclo de vida de la información, también se aplican a estos datos.

4. Biometría

La información biométrica incluye huellas dactilares, escáneres de retina, reconocimiento facial y genética. Los avances en la tecnología han aumentado enormemente los datos biométricos disponibles. Las fuerzas del orden, el sistema legal y las agencias de inteligencia han estado utilizando esta información durante mucho tiempo. Sin embargo, los datos biométricos están cada vez más disponibles en el ámbito comercial, donde pueden combinarse con otros tipos de datos, como las redes sociales. Por ejemplo, la página 45 del informe adjunto de la FTC describe un escenario en el que los minoristas pueden combinar el reconocimiento facial con las redes sociales para personalizar los mensajes a los clientes.

Todo esto abre nuevas oportunidades comerciales, así como varios problemas de gobernanza relacionados con la privacidad y la retención de datos.

5. Datos generados por humanos

Los seres humanos generan grandes cantidades de datos, como notas de los agentes del centro de llamadas, grabaciones de voz, correo electrónico, documentos impresos, encuestas y registros médicos electrónicos. Estos datos

pueden contener información confidencial que necesita ser enmascarada. Puede contener información que pueda mejorar la calidad de los conjuntos de datos estructurados y debe integrarse con MDM. Finalmente, las organizaciones deben establecer políticas con respecto al período de retención para que estos datos se adhieran a las regulaciones y administren los costos de almacenamiento.

Ahora bien, por lo que hace a la adquisición de los datos que conforman los *big data* se cuenta con el siguiente cuadro:[187]

API (Interfaz de programación de aplicaciones	Disponibles por los servicios Web, lo que les permite interactuar con ellos para examinar su contenido. Un ejemplo es la API de Twitter, la API de Facebook *Graph* y las API proporcionadas por los motores de búsqueda como Google
Software de lo que se denomina “raspado”	Realizan operaciones de rastreo, análisis y extracción de entidades para la recolección automática de datos de documentos en internet. Por ejemplo, el marco de Apache *Tika* automatiza estas operaciones para metadatos y texto de diferentes tipos de documentos, incluso identificando su idioma
La importación de información de bases de datos relacionales, no relacionales o de otras fuentes con herramientas ETL	Son ampliamente utilizadas para el manejo de datos en los sistemas Data *Warehousing* y Data *Mart*. Una de las herramientas ETL más utilizadas desde la óptica de los big data es Apache *Sqoop* que permite importar y exportar grandes cantidades de información de bases de datos relacionales y no, a la plataforma Apache Hadoop y viceversa.
Lectura de flujos de datos continuos	So n generados rápidamente, mediante sistemas capaces de capturar eventos, editarlos y guardarlos en una base de datos de manera eficiente. Entre las tecnologías más populares se encuentran *Apache Flume, Apache Kafka y Microsoft Streaminsight*.

2.3. Usos y empleos del *Big Data*.

Viktor Mayer-Schönberger manifiesta que en la era de los datos masivos, estos análisis novedosos conducirán a una oleada de percepciones y predicciones útiles. “Veremos vínculos que nunca habíamos advertido antes. Entenderemos complejas dinámicas técnicas y sociales que durante años han escapado a nuestra comprensión, pese a todos nuestros esfuerzos. Pero lo más importante es que estos análisis no causales nos ayudarán a comprender el mundo preguntando *qué* en lugar de *por qué*.[188]

[187] Véase Calderón Berra, Santiago Michele, *op. cit*. p. 19.
[188] Mayer-Schönberger, Viktor y Culier Kenneth, *Big Data, La revolución de los datos masivos*, Inglaterra, Titivillus, 2013, p. 58.

En este sentido el uso de la *data* implica necesariamente una nueva filosofía en torno a cómo nos relacionamos con la información.

Mayer asevera que "las predicciones basadas en correlaciones son el corazón de los datos masivos. Los análisis de correlación se usan con tanta frecuencia hoy en día que, a veces, no valoramos bien el avance que han supuesto. Y sus usos no van a dejar de aumentar."[189]

Por medio de *big data* podemos identificar una multiplicidad de aplicaciones tales como: usos fraudulentos de tarjetas de crédito, encontrar los mejores precios para viajar en avión, resolver problemas complejos de planeación y administración urbana, dar seguimiento con gran oportunidad y detalle a la propagación de enfermedades contagiosas, guiar acciones de las fuerzas de seguridad, autorizar o negar créditos, traducir de forma automática textos de los más variados idiomas, seguir el tráfico en las ciudades, así como mejorar el mantenimiento y control de equipos sofisticados de maquinaria, autos y aviones, entre muchas aplicaciones más.[190]

De tal suerte que gracias a las herramientas de analítica, las grandes empresas saben qué publicidad enviarnos si estamos cerca de "x" o "y" tiendas, porque tienen acceso a nuestra geolocalización; o bien, qué tiendas departamentales o aerolíneas en línea conozcan nuestras preferencias de compra; las redes sociales conozcan qué contenidos vemos con más frecuencia; y por supuesto, que el gigante Google, tenga destinados e integrados algoritmos de tal forma que nos coloquen casi intuitivamente lo que vamos a buscar.

Ahora bien, de los denominados Objetivos de Desarrollo Sostenible (ODS), la ciencia de los datos y la analítica web pueden contribuir al desarrollo sostenible de la siguiente forma:

1. Fin de la pobreza. Las tendencias de gasto en los servicios de telefonía móvil pueden proporcionar indicadores indirectos de los niveles de ingresos.
2. Hambre cero. El *crowdsourcing* o seguimiento de los precios de los alimentos en Internet puede ayudar a controlar la seguridad alimentaria casi en tiempo real.
3. Salud y bienestar. Rastrear el movimiento de los usuarios de teléfonos móviles puede ayudar a predecir la propagación de enfermedades infecciosas.

[189] *Ibidem*, p. 52.
[190] Leyva, Gerardo, *Big Data: La revolución de que no debemos Ignorar (reseña)*, en "Realidad, Datos y Espacio. Revista Internacional de Estadística y Geografía", INEGI, México, Vol 6. Num. 2, mayo-agosto 2015, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://rde.inegi.org.mx/rde_15/doctos/rde_15_opt.pdf* p. 75.

4. Educación de calidad. Las denuncias de los ciudadanos pueden descubrir las razones de las tasas de abandono escolar.
5. Igualdad de Género. El análisis de las transacciones financieras puede revelar los patrones de gasto y el diferente impacto de las crisis económicas en hombres y mujeres.
6. Agua Limpia y Saneamiento. Unos sensores conectados a las bombas de agua pueden detectar agua limpia.
7. Energía Asequible y no contaminante. Los contadores inteligentes permiten a las empresas de servicios públicos aumentar o restringir el flujo de electricidad, gas o agua para reducir el desperdicio y garantizar un suministro adecuado en los periodos álgidos.
8. Trabajo decente y crecimiento económico. Las tendencias en el tráfico postal pueden proporcionar indicadores tales como el crecimiento económico, las remesas, el comercio y el PIB.
9. Industria, innovación e infraestructura. Los datos de los dispositivos GPS se pueden usar para controlar el tráfico y mejorar el transporte público.
10. Reducción de las desigualdades. El análisis del discurso del contenido de los radios locales puede revelar problemas de discriminación y respaldar la adopción de políticas de respuesta.
11. Ciudades y comunidades sostenibles. La teleobservación por medio de satélites puede rastrear la intrusión en tierras o espacios públicos, como parques y bosques.
12. Producción y consumo responsables. Los patrones de búsqueda en línea o las transacciones de comercio electrónico pueden revelar el ritmo de la transición a productos energéticamente eficientes.
13. Acción por el Clima. La combinación de las imágenes de satélite, los testimonios de personas y los datos de libre acceso puede ayudar a rastrear la deforestación.
14. Vida Submarina. Los datos de seguimiento de los buques marítimos pueden evidenciar actividades de pesca ilegales, no reguladas y no declaradas.
15. Vida de Ecosistemas terrestres. Las redes sociales pueden ayudar a gestionar los desastres con información instantánea sobre la ubicación de las víctimas, los efectos y la intensidad de los incendios forestales o la neblina.
16. Paz, Justicia e Instituciones Sólidas. El análisis de las emociones en las redes sociales puede mostrar la opinión pública en temas como la gobernanza eficaz, la prestación de servicios públicos o los derechos humanos.
17. Alianzas para lograr los objetivos. Las colaboraciones para permitir la combinación de estadísticas, datos móviles y de Internet pueden proporcionar una mejor comprensión -y en tiempo real- del mundo hiper conectado en el que vivimos.[191]

[191] Organización de las Naciones Unidas, *Macrodatos y los ODS. Cómo la ciencia de datos y la*

Por su parte, Carlos Antonio Osorio comenta que el empleo del *big data* puede generar diferentes tipos beneficios tanto empresariales como industriales, tal como se muestra a continuación: [192]

Beneficios empresariales:

1. Encontrar rápidamente oportunidades de mejora en las áreas de la empresa y minimizar el error humano.
2. Rapidez en la toma de decisiones asertivas
3. Mejor conocimiento de los clientes
4. Reducción de costos y optimización de procesos

Beneficios en el Sector energético y servicios públicos:

1. Predicción de producción de energía renovable.
2. Análisis de datos para detección de fallas y mantenimientos preventivos.
3. Predecir el consumo de energía para gestionar la demanda y la oferta.
4. Detección de fraudes en los consumos de los usuarios.
5. Definición de patrones de consumo versus generación de energía.

Beneficios en la industria del *Retail*:

1. Plataformas de escucha basadas en Big Data, donde los flujos de datos de las redes sociales se filtran y analizan en busca de ciertas palabras clave o sentimientos de los consumidores hacia la marca.
2. Predicción de visitantes para la optimización de la sección de cajas.

Beneficios Industria y manufactura:

1. Pronóstico de inventario para optimizar el proceso de producción.
2. Monitoreo del rendimiento de las máquinas, predicción de fallas y mantenimiento preventivo.

Beneficios en las Tics:

1. Rastreo del rendimiento y usabilidad del sitio web.
2. Análisis de grandes volúmenes de datos proveniente de campañas de marketing digital para predecir el comportamiento de productos nuevos.

Beneficios en Otros sectores:

1. Las agencias de publicidad lo utilizan para diseñar campañas de marketing más específicas y rápidas.
2. Los diseñadores de moda lo usan para seguir tendencias y crear productos más innovadores.

---

analítica web pueden contribuir al desarrollo sostenible, ONU, 2018, Global Pulse, Secc. Desafíos Globales [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.un.org/es/global-issues/big-data-for-sustainable-development*

[192] Osorio Gómez, Carlos Antonio, *Beneficios y Usos del Big Data*, Revista Empresarial y Laboral, Secc. Tendencias Edición On Line, Colombia, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://revistaempresarial.com/tecnologia/tendencias/beneficios-y-usos-del-big-data/*

3. Los Bancos usan las tendencias para hacer inversiones más efectivas y rentables.

2.3.1. Minería de Datos

En este entorno tan lleno de datos, es necesario conocer las medidas de almacenamiento de datos como se muestra a continuación:[193]

1 bit es la unidad mínima de almacenamiento.
8 bits = 1 byte.
1024 bytes = 1 kilobyte.
1024 kilobytes = 1 megabyte.
1024 megabytes = 1 gigabyte.
1024 gigabytes = 1 terabyte.
1024 terabytes = 1 petabyte.
1024 petabyte = 1 exabyte.
1024 exabytes = 1 zettabyte.
1024 zettabyte = 1 yottaByte.
1024 yottabytes = 1 brontobyte.
1024 brontobytes = 1 geopbyte

Esther Riveroll, Directora General de *All datum Business* comentó que "El 90% de la data del mundo se creó en los últimos dos años. En 2018 surgieron 33 ZB de datos y de estos el 86% fue creado de copias y distribución de los mismos. Se está generando una cantidad enorme de información día a día y debe existir una estrategia para poder administrar, almacenar, analizar y obtener valor de todo lo que actualmente se está generando. Hoy en día sabemos que mientras más datos, más análisis y mejores resultados"[194]

Todo este volumen de datos, de puede utilizar de manera disgregada, o bien mediante bases de datos.

Una base de datos "es un conjunto de datos almacenados en memoria externa que están organizados mediante una estructura de datos. Cada base de datos ha sido diseñada para satisfacer los requisitos de información de una empresa u otro tipo de organización, como, por ejemplo, una universidad o un hospital". [195]

Para Rafael Camps, una base de datos es "la representación integrada de los

[193] Tascón Mario, y Coullaut Arantza, *Big Data y el internet de las Cosas. Qué hay detrás y cómo nos va a cambiar,* España, Catarata, 2016, p. 74.
[194] Citada por Nieto, Anahí, *Big Data, una tendencia con Negocios Exponenciales*, Revista eSemanal, [en línea] México, Sec. Reportaje, Año. 29, No. 1403, 9 de noviembre de 2020, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://esemanal.mx/ejemplares/1403/1403.pdf* p. 7.
[195] Marqués, Mercedes, *Bases de Datos*, [en línea] España, *Universitat* Jaime I, 2011, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://bdigital.uvhm.edu.mx/wp-content/uploads/2020/05/Bases-de-Datos.pdf* p. 1.

conjuntos de entidades instancia correspondientes a las diferentes entidades tipo del SI [Sistema Inteligente] y de sus interrelaciones. Esta representación informática (o conjunto estructurado de datos) debe poder ser utilizada de forma compartida por muchos usuarios de distintos tipos. En otras palabras, una base de datos es un conjunto estructurado de datos que representa entidades y sus interrelaciones."[196]

Por su parte, Gómez Fuentes menciona que el término base de datos surgió en 1963, cuando en la informática, una base de datos consistía en una "colección de datos interrelacionados y un conjunto de programas para acceder a dichos de datos. En otras palabras, una base de datos no es más que un conjunto de información (un conjunto de datos) relacionada que se encuentra agrupada o estructurada."[197]

Antes del uso de las bases de datos lo común es que es emplearan los archivos para guardar la información; sin embargo, ante la acumulación de la información, comenzaron a presentarse diferentes problemas tal como lo menciona Silberschatz:

- Redundancia e inconsistencia de los datos.- Redundancia significa tener el mismo dato guardado varias veces. Inconsistencia significa que hay contradicción en el contenido de un mismo dato, es decir, que un mismo dato tiene un valor en una parte de la memoria, mientras que en otra parte contiene otro valor diferente.
- Dificultad en el acceso a los datos.- Era difícil que el usuario encontrara rápidamente un dato en especial.
- No existía el aislamiento de los datos.- Debido a que los datos estaban dispersos en varios archivos y podían estar en diferentes formatos, era difícil escribir programas nuevos de aplicación para recuperar los datos apropiados.
- Problemas de integridad.- Era complicado asegurarse que los valores almacenados satisficieran ciertos tipos de restricciones, por ejemplo, que tuvieran un valor mínimo y/o un valor máximo.
- Problemas de atomicidad.- Era muy difícil asegurar que una vez que haya ocurrido alguna falla en el sistema y se ha detectado, los datos se restaurarán al estado de consistencia que existía entes de la falla.
- Anomalías en el acceso concurrente.- La cuestión de asegurar la consistencia de los datos se complica todavía más cuando se trata de sistemas en los que hay varios usuarios accediendo a un mismo archivo desde diferentes computadoras.

[196] Camps Paré, Rafael, *Software Libre*, [en línea] España, *Univiersitat* Oberta de Catalunya, 2005, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.uoc.edu/pdf/masters/oficiales/img/913.pdf* p. 8.
[197] Gómez Fuentes, María del Carmen, *Material Didáctico, Notas del Curso Bases de Datos*, [en línea] México, UAM Cuajimalpa, 2013, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *http://www.cua.uam.mx/pdfs/conoce/libroselec/Notas_del_curso_Bases_de_Datos.pdf* p. 5.

- Problemas de seguridad.- No todos los usuarios de un sistema de información deberían poder acceder a todos los datos. En un sistema de archivos es muy difícil garantizar las restricciones de seguridad.[198]

Todas estas problemáticas, ocasionaron el desarrollo de los sistemas de bases de datos o también llamados Sistemas de Gestión de Bases de Datos (SGBD). Un sistema de administración de bases de datos es una "herramienta de propósito general que permite crear bases de datos de cualquier tamaño y complejidad y con propósitos específicos distintos."[199]

Con el desarrollo tecnológico de los softwares y lenguajes empleados en las bases de datos, la gestión de las mismas y su empleo por parte de empresas y organizaciones es de vital importancia. Algunas de las aplicaciones más representativas de las bases de datos son las siguientes:

- Bancos.- Para información de los clientes, cuentas, préstamos y transacciones bancarias.
- Líneas aéreas.- para reservas e información de planificación.
- Universidades.- Para información de los estudiantes, de los profesores y de los cursos.
- Tarjetas de crédito.- Para compras con tarjetas de crédito y generación de estados de cuenta.
- Telecomunicaciones.- Para llevar registro de las llamadas realizadas, generación mensual de facturas, mantenimiento del saldo de las tarjetas telefónicas de prepago, para almacenar información sobre las redes de comunicaciones.
- Finanzas.- Para almacenar información sobre grandes empresas, ventas y compras de documentos financieros como bolsa y bonos.
- Ventas.- Para información de clientes, productos y compras.
- Producción.- Para la administración de la cadena de producción (inventarios, pedidos, etc.).
- Recursos humanos.- Para información sobre los empleados, salarios, impuestos, prestaciones y para la generación de nóminas.[200]

Las bases de datos pueden protegerse vía derechos de autor; la Directiva 96/9/CE sobre la protección jurídica de las bases de datos tiene como objetivo brindar protección jurídica a las bases de datos, articulada en dos aspectos:

- Protección de los derechos de autor para la creación intelectual relacionada con la selección o disposición de materiales;

[198] *Ibidem*, pp. 6-7.
[199] *Ibidem*, p. 5.
[200] *Ibidem*, p. 7.

- Protección *sui generis* de una inversión cuantiosa (financiera o entendida en términos de recursos humanos, esfuerzo y energía) efectuada para la obtención, la verificación o la presentación del contenido de una base de datos.[201]

Esta Directiva se ha revisado en dos ocasiones, una en 2005, otra en 2018 y recientemente, para este 2021, se realizará otra revisión a la misma.

En México las bases de datos se encuentran protegidas en la Ley Federal del Derecho de Autor (LFDA). El artículo 107 dispone que las bases de datos o de otros materiales legibles por medio de máquinas o en otra forma, que por razones de selección y disposición de su contenido constituyan creaciones intelectuales, quedarán protegidas como compilaciones. Dicha protección no se extenderá a los datos y materiales en sí mismos.

En este sentido, dado que los datos *per se* no estarán protegidos por la LFDA, en el caso de los Datos Personales estarán protegidos por las leyes de datos personales en México, de las cuales se hablará en el apartado respectivo.

El manejo de los datos y por ende de la información es totalmente abstracto, las bases de datos ayudan a integrar y simplificar la búsqueda de la información de una forma más o menos íntegra y segura. Sin embargo, ahora existen diferentes bases de datos con capacidades de almacenamiento inconmensurables. Por ello, es que la figura de la minería de datos sale al rescate con el objetivo de buscar una aguja en un pajar.

La minería de datos "es el proceso que tiene como propósito descubrir, extraer y almacenar información relevante de amplias bases de datos, a través de programas de búsqueda e identificación de patrones y relaciones globales, tendencias, desviaciones y otros indicadores aparentemente caóticos que tienen una explicación que pueden descubrirse mediante diversas técnicas de esta herramienta."[202]

Yolanda Belinchón menciona que minería de datos es "todo conjunto de técnicas encargas (*sic*) de la extracción de conocimiento procesable, implícito en las bases de datos (ayuda a comprender su contenido). Está fuertemente ligada con la supervisión de procesos industriales, pues resulta muy útil para aprovechar los datos almacenados en las bases de datos."[203]

---

[201] Parlamento Europeo, *Protección Jurídica: Bases de datos*, [en línea], [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://eur-lex.europa.eu/legal-content/ES/LSU/?uri=CELEX:31996L0009*

[202] Ángeles Larrieta, María Isabel y Santillán Gómez, Angélica María, *Minería de datos: Concepto, características, estructura y aplicaciones*, UNAM, México, Revista de Contaduría y Administración, 06 de mayo de 2003, http://www.ejournal.unam.mx/rca/190/RCA19007.pdf p. 79.

[203] Belinchón Monjas, Yolanda, *Minería de Datos*, Universidad Carlos III de España, España, s/d http://www.it.uc3m.es/jvillena/irc/practicas/10-11/15mem.pdf p. 1.

El análisis mediante minería de datos se lleva a cabo con dos actividades para obtener conocimiento no conocido: a) describir en detalle a los generadores de datos, y b) predecir su comportamiento en su entorno; todo esto utilizando la historia almacenada en la bodega de datos.

La descripción en detalle se hace a partir de una revisión exhaustiva de toda la información disponible, revisión que también permite conocer a los generadores de datos en cada momento. Y conocer el comportamiento de los generadores puede ayudar a las personas que toman decisiones a identificar futuras situaciones deseadas o no deseadas, aun con datos faltantes, y poder indicar el valor de éstos con cierta certidumbre.[204]

Algunas de las tareas importantes de la minería de datos incluyen la identificación de aplicaciones para las técnicas existentes, y desarrollar nuevas técnicas para dominios tradicionales o de nueva aplicación, como el comercio electrónico y la bioinformática. Existen numerosas áreas donde la minería de datos se puede aplicar, prácticamente en todas las actividades humanas que generen datos:[205]

- Comercio y banca: segmentación de clientes, previsión de ventas, análisis de riesgo.
- Medicina y Farmacia: diagnóstico de enfermedades y la efectividad de los tratamientos.
- Seguridad y detección de fraude: reconocimiento facial, identificaciones biométricas, accesos a redes no permitidos, etc.
- Recuperación de información no numérica: minería de texto, minería web, búsqueda e identificación de imagen, video, voz y texto de bases de datos multimedia.
- Astronomía: identificación de nuevas estrellas y galaxias.
- Geología, minería, agricultura y pesca: identificación de áreas de uso para distintos cultivos o de pesca o de explotación minera en bases de datos de imágenes de satélites.
- Ciencias Ambientales: identificación de modelos de funcionamiento de ecosistemas naturales y/o artificiales (p.e. plantas depuradoras de aguas residuales) para mejorar su observación, gestión y/o control.
- Ciencias Sociales: Estudio de los flujos de la opinión pública. Planificación de ciudades: identificar barrios con conflicto en función de valores sociodemográficos.

[204] Martínez Luna, Gilberto Lorenzo, *op. cit.* p. 24.
[205] Riquelme, José C. *et. al*. *Minería de Datos, Conceptos y Tendencias*, Revista Iberoamericana de Inteligencia Artificial, [en línea] España, vol. 10, núm. 29, primavera, Inteligencia Artificial, 2006, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.redalyc.org/pdf/925/92502902.pdf* p. 14

2.4. Tecnologías de la Información y *Big Data*

Desde que el hombre comenzó a pintar una pared en una cueva se puede decir que es el nacimiento del manejo de la información; si bien de forma rupestre, marcó el inicio del uso del lenguaje con la tecnología que se tenía al alcance. Posteriormente con el advenimiento de la escritura y de los "idiomas", las diferentes culturas comenzaron a emplear diferentes mecanismos e instrumentos para dar a conocer la información de diferentes maneras y con las tecnologías que en cada época de la historia se va manejando.

Hoy por hoy con la aceleración de la llamada sociedad de la información, donde el uso de las herramientas digitales y computacionales son cada vez más indispensables, el protagonismo que la tecnología ha logrado y avanzado en cuanto a alcances y niveles de almacenamientos y desarrollo; es tal su importancia que la tecnología y la información han favorecido la integración de mercados y el uso de análisis más y más complejos.

La Sociedad de la Información es el estado en el que se encuentran las sociedades en las que se implanta y se generaliza el uso de las Tecnologías de la Información y la Comunicación en los distintos ámbitos de la vida de los ciudadanos, de las empresas y las instituciones, y que les permite acceder a la información y productos que se encuentran en formato electrónico sin limitaciones de tiempo y espacio.[206]

Las Naciones Unidas en su resolución A/RES/56/183 de fecha 31 de enero de 2002 resolvió reconocer la resolución aprobada por el Consejo de la Unión Internacional de Telecomunicaciones en su período de sesiones de 2001, en la que apoya la propuesta del Secretario General de la Unión de celebrar la Cumbre Mundial sobre la Sociedad de la Información en dos etapas: la primera en Ginebra, del 10 al 12 de diciembre de 2003, y la segunda en Túnez, en 2005.[207]

El objetivo de la primera fase en Ginebra (10-12 de diciembre de 2003) era redactar y propiciar una clara declaración de voluntad política, y tomar medidas concretas para preparar los fundamentos de la Sociedad de la Información para todos, que tenga en cuenta los distintos intereses en juego. De esta cumbre se emitieron la Declaración de Principios de Ginebra y el Plan de Acción de Ginebra, que se aprobaron el 12 de diciembre de 2003.

El objetivo de la segunda fase en Túnez (16-18 de noviembre de 2005) fue poner en marcha el Plan de Acción de Ginebra y hallar soluciones y alcanzar acuerdos en

[206] Ayala Ñiquen, Evelyn Elizabeth, y Gonzáles Sánchez, Santiago Raúl, *Tecnologías de la Información y la Comunicación*, [en línea] Perú, Universidad Inca Garcilaso de la Vega, 2015, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *http://repositorio.uigv.edu.pe/bitstream/handle/20.500.11818/1189/Libro%20TIC%20%282%29-1-76%20%281%29.pdf?sequence=1&isAllowed=y* p. 21.

[207] Organización de las Naciones Unidas, *Resolución 56/183 Cumbre Mundial sobre la Sociedad de la Información*, [en línea] ONU, 2002, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.itu.int/net/wsis/docs/background/resolutions/56_183_unga_2002-es.pdf* p.2.

los campos de gobierno de Internet, mecanismos de financiación y el seguimiento y la aplicación de los documentos de Ginebra y Túnez. De esta cumbre se emitieron el Compromiso de Túnez y al Programa de Acciones de Túnez para la Sociedad de la Información, que se aprobaron el 18 de noviembre de 2005.

Al término de estas dos fases, la Unión Internacional de Telecomunicaciones emitió los documentos finales sobre la Cumbre Mundial sobre la Sociedad de la Información donde se plasmaron los acuerdos tomados tanto en Ginebra en 2003, cómo en Túnez en 2005.[208]

La Declaración de Principios de Ginebra contempló tres puntos principales:

1. Nuestra visión común de la Sociedad de la Información.
    a. Basada en promover los objetivos de la entonces Declaración del Milenio encauzando el potencial de la tecnología de la información y la comunicación.
    b. Reconocen una visión integradora y orientada al desarrollo, en que todos puedan crear, consultar, utilizar y compartir la información y el conocimiento, para que las personas, las comunidades y los pueblos puedan emplear plenamente sus posibilidades en la promoción de su desarrollo sostenible y en la mejora de su calidad de vida.
    c. Se afirmó que el desarrollo de las TIC brinda ingentes oportunidades a las mujeres.
    d. Se contempló también que en la evolución de la Sociedad de la Información, se debe prestar particular atención a la situación especial de los pueblos indígenas, así como a la preservación de su legado y su patrimonio cultural.
2. Una Sociedad de la Información para todos: Principios fundamentales.
    a. La función de los gobiernos y de todas las partes interesadas en la promoción de las TIC para el desarrollo
    b. Infraestructura de la Información y las comunicaciones: fundamento básico de una Sociedad de la Información integradora.
    c. Acceso a la Información y al conocimiento.
    d. Creación de capacidades.
    e. Fomento de la confianza y seguridad en la utilización de las TIC.
    f. Entorno Propicio.
        i. El estado de derecho, acompañado por un marco de política y reglamentación propicio, transparente, favorable a la competencia, tecnológicamente neutro, predecible y que refleje

[208] Unión Internacional de Telecomunicaciones, *Cumbre Mundial sobre la Sociedad de la Información, Documentos Finales, Ginebra 2003-Túnez 2005*, [en línea] UIT, Ginebra, 2005, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.itu.int/net/wsis/outcome/booklet-es.pdf* p. 1.

las realidades nacionales, es insoslayable para construir una Sociedad de la Información centrada en la persona.

ii. Las TIC son un importante factor que propicia el crecimiento, ya que mejoran la eficacia e incrementan la productividad, especialmente en las pequeñas y medianas empresas (PYME).

iii. La protección de la propiedad intelectual es importante para alentar la innovación y la creatividad en la Sociedad de la Información, así como también lo son una amplia divulgación, difusión e intercambio de los conocimientos.

g. Aplicaciones de las TIC: Beneficios en todos los aspectos de la vida.

i. Las aplicaciones TIC son potencialmente importantes para las actividades y servicios gubernamentales, la atención y la información sanitaria, la educación y la capacitación, el empleo, la creación de empleos, la actividad económica, la agricultura, el transporte, la protección del medio ambiente y la gestión de los recursos naturales, la prevención de catástrofes y la vida cultural, así como para fomentar la erradicación de la pobreza.

h. Diversidad e identidad culturales, diversidad lingüística y contenido local.

i. La Sociedad de la Información debe fundarse en el reconocimiento y respeto de la identidad cultural, la diversidad cultural y lingüística, las tradiciones y las religiones, además de promover un diálogo entre las culturas y las civilizaciones.

i. Medios de comunicación.

i. Se busca que los medios de comunicación utilicen y traten la información de manera responsable, de acuerdo con los principios éticos y profesionales más rigurosos.

j. Dimensiones éticas de la Sociedad de la información.

i. La importancia de la ética para la Sociedad de la Información debe fomentar la justicia, así como la dignidad y el valor de la persona humana.

ii. Los actores de la Sociedad de la Información deben adoptar las acciones y medidas preventivas apropiadas, con arreglo al derecho, para impedir la utilización abusiva de las TIC.

k. Cooperación internacional y regional.

i. La Sociedad de la Información es por naturaleza intrínsecamente global y los esfuerzos nacionales deben ser respaldados por una cooperación eficaz, a nivel internacional y regional entre los gobiernos, el sector privado, la sociedad civil y las demás partes interesadas, entre ellas, las instituciones financieras internacionales.

3. Hacia una Sociedad de la Información para todos, basada en el Intercambio de Conocimientos.
    a. Se busca reducir las brechas digitales.

El Plan de Acción de Ginebra tienen los siguientes puntos:

1. Introducción.
    a. Se reconoce que el gobierno, el sector privado, el sector social y diferentes instituciones internacionales y regionales puedan prestar una contribución importante en la Sociedad de la Información.
2. Objetivos y metas.
    a. Construir una Sociedad de la Información integradora, poner el potencial del conocimiento y las TIC al servicio del desarrollo, fomentar la utilización de la información y del conocimiento para la consecución de los objetivos de desarrollo acordados internacionalmente.
    b. Establecer objetivos de ciberestrategias nacionales y de conformidad con las políticas de desarrollo nacionales.
3. Líneas de acción.
    a. El papel de los gobiernos y de todas las partes interesadas en la promoción de las TIC para el desarrollo.
    b. Infraestructura de la Información y la comunicación: fundamento básico para la sociedad de la información.
    c. Acceso a la información y al conocimiento.
    d. Creación de capacidades.
    e. Creación de confianza y seguridad en la utilización de las TIC.
    f. Entorno habilitador.
    g. Aplicaciones de la TIC: ventajas en todos los aspectos de la vida.
        i. Gobierno Electrónico.
        ii. Negocios Electrónicos.
        iii. Aprendizaje electrónico.
        iv. Cibersalud.
        v. Ciberempleo.
        vi. Ciberecología.
        vii. Ciberagricultura.
        viii. Ciberciencia.
    h. Diversidad e identidad culturales, diversidad lingüística y contenido local.
    i. Medios de comunicación.
    j. Dimensiones éticas de la Sociedad de la Información.
    k. Cooperación internacional y regional.
4. Agenda de Solidaridad Digital.
5. Seguimiento y evaluación.
6. Hacia una segunda fase de la CMSI (Túnez)

Por su parte la Agenda de Túnez para la Sociedad de la Información contempló los siguientes puntos:

1. Introducción.
2. Mecanismos de financiación para hacer frente a los retos de las TIC para el desarrollo.
3. Gobernanza de Internet.
    a. La gestión internacional de Internet debería ser multilateral, transparente y democrática, y hacerse con la plena participación de los gobiernos, el sector privado, la sociedad civil y las organizaciones internacionales.
    b. La gobernanza de Internet, llevada a cabo con arreglo a los Principios de Ginebra, es un elemento esencial de una Sociedad de la Información centrada en la persona, integradora, orientada al desarrollo y no discriminatoria.
    c. La gobernanza de Internet es ***desarrollo y aplicación por los gobiernos, el sector privado y la sociedad civil, en el desempeño de sus respectivos papeles, de principios, normas, reglas, procedimientos de toma de decisiones y programas comunes que dan forma a la evolución y a la utilización de Internet***.
    d. Se debe garantizar el respeto por la privacidad y la protección de los datos e informaciones personales, ya sea mediante la adopción de medidas legislativas y la aplicación de marcos de colaboración, o bien mediante el intercambio entre las empresas y los usuarios de mejores prácticas, mecanismos de autorregulación o medidas tecnológicas pertinentes.
4. Implementación y seguimiento

Por su parte, el Foro de la Cumbre Mundial sobre la Sociedad de la Información 2021 llevada a cabo en línea entre enero y mayo, representa la mayor reunión anual del mundo de la comunidad de las "TIC para el desarrollo". El Foro de la CMSI, organizado conjuntamente por la UIT, la UNESCO, el PNUD y la UNCTAD, en estrecha colaboración con todos los facilitadores/cofacilitadores de las líneas de acción de la CMSI, ha demostrado ser un mecanismo eficaz para la coordinación de las actividades de aplicación de las múltiples partes interesadas, el intercambio de información, la creación de conocimientos, el intercambio de las mejores prácticas y sigue prestando asistencia en la creación de asociaciones de múltiples partes interesadas y públicas/privadas para avanzar en los objetivos de desarrollo.[209]

Dentro de los puntos tratados en esta cumbre de 2021 están:

[209] Unión Internacional de Telecomunicación, *Foro de la Cumbre Mundial sobre la Sociedad de la Información 2021*, [Versión HTML], s/d, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.itu.int/net4/wsis/forum/2021/es*

1. Las TIC y la incorporación de la perspectiva de género. El tema de las TIC y la integración de la perspectiva de género está dedicado a las cuestiones de la reducción de la brecha de género, el empoderamiento de las mujeres y la promoción de la perspectiva de igualdad a través del uso de las TIC.
2. Las TIC y la juventud. Poner de relieve la necesidad de que las comunidades juveniles de la CMSI sigan promoviendo el papel indispensable de las TIC en la configuración de la sociedad de la información para servir mejor a todas las partes interesadas, responder adecuadamente a la pandemia actual y seguir transformando digitalmente el desarrollo social, económico y medioambiental.
3. Las TIC y las personas mayores. Aborda el papel de la tecnología para lograr un envejecimiento más saludable, pero también cómo la tecnología puede ayudarnos a construir ciudades más inteligentes, a combatir la discriminación por motivos de edad en el lugar de trabajo, a garantizar la inclusión financiera de las personas mayores y a apoyar a millones de cuidadores en todo el mundo.
4. Las TIC y la accesibilidad para las personas con discapacidad y necesidades específicas. Este tema pretende informar y observar cómo las TIC pueden ayudar a las personas con discapacidad, centrándose al mismo tiempo en el progreso hacia los Objetivos de Desarrollo Sostenible de las Naciones Unidas.
5. Ciberseguridad. Este nuevo tema incluirá sesiones que se ajustan a la Línea de Acción C5 de la CMSI: Crear confianza y seguridad en el uso de las TIC. La ciberseguridad es crucial para garantizar un acceso universal, fiable y equitativo a la conectividad.
6. Tecnologías emergentes para el desarrollo sostenible (Startups). Las tecnologías emergentes están llamadas a tener un impacto vital en nuestro futuro. La Inteligencia Artificial, la Realidad Aumentada y el Big Data ya están demostrando tener un inmenso potencial en sectores como la sanidad, la educación, la agricultura y muchos más.
7. Las TIC para el bienestar y la felicidad. El bienestar puede estar sujeto a la salud, la felicidad y la prosperidad, y puede atribuirse a cinco tipos como el bienestar emocional, el bienestar físico, el bienestar social, el bienestar en el lugar de trabajo y el bienestar de la sociedad. En este periodo de distanciamiento social forzoso en el que uno está atado a su casa, la vida rutinaria puede volverse mundana y, por tanto, puede resultar difícil estar en paz. El tema de las TIC para el bienestar y la felicidad traerá una serie de talleres centrados en los esfuerzos y los éxitos para promover una vida sana y el bienestar para todos en todas las edades, en el contexto de la pandemia COVID-19.

Una vez tratada la parte de la Sociedad de la información, es momento de abordar específicamente el tema de las Tecnologías de la Información. Sobre el particular, existen diferentes opiniones respecto a si el concepto adecuado es el de

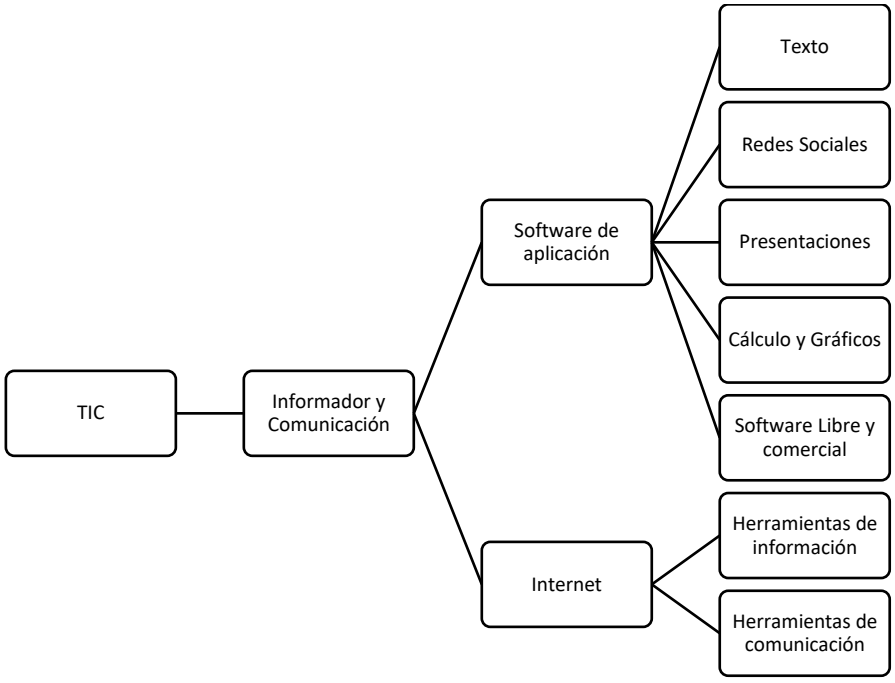
Tecnologías de la Información o el de Tecnologías de la Información y la Comunicación.

Para Ayala Ñíguen, las tecnologías de la información y la comunicación (TIC) son el "conjunto de tecnologías que permiten el acceso, producción, tratamiento y comunicación de información presentada en diferentes códigos (texto, imagen, sonido, video)."[210]

Continúa comentando Ayala, que las TIC es un término que contempla "toda forma de tecnología usada para: crear, almacenar, intercambiar y procesar información en sus varias formas, tales como: datos, conversaciones de voz, imágenes fijas o en movimiento, presentaciones multimedia y otras formas, incluyendo aquéllas aún no concebidas. Su objetivo principal es la mejora y el soporte a los procesos de operación y negocios para incrementar la competitividad y productividad de las personas y organizaciones en el tratamiento de cualquier tipo de información."[211]

Por su parte Jorge Vasconcelos, indica que el concepto de Tecnologías de la Información (él le retira el de comunicación) es el "conjunto de dispositivos, servicios y actividades apoyadas por equipo de cómputo, y que se basan en la transformación de información numérica, también llamada digital."[212]

Para Vasconcelos la estructura conceptual de las TIC es la siguiente:[213]



[210] Ayala Ñiquen, Evelyn Elizabeth, y Gonzáles Sánchez, Santiago Raúl, *op. cit*. p. 27.
[211] *Ibidem*. p. 28.
[212] Vasconcelos Santillán, Jorge, *Tecnologías de la Información*, México, Patria, 2da ed., 2015, p. 2
[213] *Ibidem*. p. IX.

Imagen: Estructura conceptual de las TIC.
Tomada de: Vasconcelos Santillán, Jorge, Tecnologías de la Información, México, Patria, 2da ed, 2015, p. IX.

Las TIC sin lugar a dudas evolucionan constantemente, tan solo en el desarrollo del software, han aparecido una serie de herramientas con funcionalidades y aplicaciones de diferente índole como:

- Intranet: Red privada de una organización diseñada y desarrollada siguiendo los protocolos propios y el funcionamiento de Internet, protocolo TCP/IP, navegador web. Su utilización es interna, pero puede estar conectada a Internet y a otras redes externas. Para los usuarios, se resume en una serie de páginas Web que dan acceso a la distinta documentación de la empresa, informaciones corporativas, aplicaciones informáticas, incluso permiten la publicación de información y conocimientos personales de cada empleado. Además, dentro de Intranet se pueden organizar y tener acceso a comunidades de prácticas virtuales, foros y listas de distribución.
- Software de simulación y realidad virtual: Aplicaciones que permiten minimizar los costes de la realización de prototipos, experimentar nuevas ideas y simular la aplicación de conocimientos.
- Videoconferencias: Sistema que permite a varias personas, con independencia de su ubicación geográfica, entablar, mediante aplicaciones específicas, una conversación con soporte audio y video en tiempo real.
- *Datamining*: Tecnología que permite la explotación y análisis de los datos almacenados por la organización, generalmente una gran cantidad de datos almacenados en bases de datos y *datawarehouse*, buscando entre ellos relaciones y patrones de comportamiento no observables directamente.
- *Datawarehouse*: Repositorio o almacén de datos de gran capacidad que sirve de base común a toda la organización. Almacena los datos procedentes tanto del interior de la organización como del exterior, organizándolos por temas, lo que facilita su posterior explotación.
- Inteligencia artificial: Aplicaciones informáticas a las que se dota de propiedades asociadas a la inteligencia humana. Ejemplos son los sistemas expertos, redes neuronales; que a partir del conocimiento y reglas introducidas por un experto humano permiten alcanzar inferencia y resolver problemas.
- Motores de búsqueda: Software diseñado para rastrear fuentes de datos, tales como: bases de datos, Internet; lo que permite indexar su contenido y facilitar su búsqueda y recuperación.
- Gestión documental: Aplicaciones que permiten la digitalización de documentos, su almacenamiento, el control de versiones y su disponibilidad para los usuarios con autorización para su consulta o modificación.
- Mapas de conocimiento y páginas amarillas: Directorios que facilitan la localización del conocimiento dentro de la organización mediante el

desarrollo de guías y listados de personas, o documentos, por áreas de actividad o materias de dominio.

- Mensajería instantánea y correo electrónico: Aplicaciones que facilitan la comunicación en tiempo real o diferido, así como el intercambio de documentos.
- *Groupware*: Tecnologías diseñadas para la gestión de trabajos en equipo. Facilita la coordinación en el trabajo y compartir informaciones y aplicaciones informáticas.[214]

Una de las formas en las que las TIC han venido a revolucionar es también en el Gobierno. Hoy cada vez es más fácil hablar de Gobierno Electrónico.

El Gobierno Electrónico es definido por la OEA como "el uso de las Tecnologías de Información y Comunicación TIC, por parte de las instituciones de gobierno, para mejorar cualitativamente los servicios e información que se ofrecen a los ciudadanos; aumentar la eficiencia y eficacia de la gestión pública e incrementar sustantivamente la transparencia del sector público y la participación ciudadana."[215]

Este concepto reúne los siguientes atributos relativos a la aplicación del gobierno electrónico: Implica innovación en las relaciones internas y externas del gobierno con:

- Otras agencias gubernamentales
- Sus propios empleados.
- Las empresas y el ciudadano.

Tiene implicaciones sobre la organización y función del gobierno en lo que se refiere a los siguientes aspectos:

- Acceso a la información
- Prestación de servicios y realización de trámites
- Participación ciudadana
- Busca optimizar el uso de los recursos para el logro de los objetivos trazados
- Su implementación implica el paso por una serie de estados (o fases), no necesariamente consecutivos
- Es un medio, no un fin en sí mismo

Se puede hablar de una sucesión de fases dentro del proceso de implementación del gobierno electrónico, las cuales no son, en todos los casos, necesariamente consecutivas. Observar los alcances y beneficios que surgen del avance de las herramientas de gobierno electrónico a una fase de mayor desarrollo, pone en evidencia su capacidad de mejorar la eficiencia y la transparencia de las

[214] Ayala Ñiquen, Evelyn Elizabeth, y Gonzáles Sánchez, Santiago Raúl, *op. cit*. p. 37.
[215] Organización de Estados Americanos, *Guía de Mecanismos para la Promoción de la Transparencia*
y la Integridad en las Américas, [en línea] OEA, Departamento para la Gestión Pública Efectiva, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.oas.org/es/sap/dgpe/guia_egov.asp*

instituciones públicas.

En términos generales, las que se conocen como fases de gobierno electrónico se han denominado de la siguiente manera.[216]

I. Presencia
II. Interacción
III. Transacción
IV. Transformación
V. Participación democrática

Fase I - Presencia: Muchas empresas del sector público se encuentran en esta etapa, en la que se limitan a utilizar las TIC para ofrecer información básica al público.

Fase II - Interacción: En la segunda fase, se amplía la capacidad de las empresas de ofrecer servicios a través de las TIC, de tal manera que el ciudadano puede acceder a información crítica, diligenciar formatos que puede obtener de la Web y establecer contacto vía correo electrónico. Hasta este nivel ya han llegado una gran cantidad de instituciones.

Fase III - Transacción: En esta fase, en la que se encuentran instituciones más avanzadas en materia de tecnología, se han incorporado aplicaciones de auto servicio para que el ciudadano pueda realizar trámites completos en línea.

Fase IV - Transformación: Consiste en una integración total entre agencias, el sector privado y la ciudadanía, ofreciendo servicios cada vez más personalizados. En esta etapa surgen conceptos como el de ventanilla Única, y sistemas de agencias cruzadas con servicios compartidos.

Fase V – Participación Democrática: Se refiere a la posibilidad de utilizar herramientas de gobierno electrónico para el ejercicio de derechos ciudadanos, como, por ejemplo, el voto electrónico y el acceso a información sobre acciones y decisiones de los gobernantes elegidos.[217]

El gobierno electrónico ha revolucionado la forma de entregar servicios y mejorar las relaciones con los ciudadanos como empresas y empleados, logrando ser visto a través de cuatro tipos de relaciones:

Gobierno a ciudadano (G2C). Son los portales institucionales de e-gobierno que proveen información a la ciudadanía sobre servicios administrativos, proporcionan información básica sobre trámites a través de las TIC desde cualquier lugar con conexión a Internet las 24 horas del día. El hecho de ofrecer servicios 7x24 permite reducir plazos, simplificar trámites y abatir barreras geográficas y de tiempo para las instituciones y la ciudadanía.

[216] *Ídem*.
[217] *Ídem*.

Gobierno a empresa (G2B). Son los portales encargados de brindar servicios administrativos y de información al sector empresarial. Los beneficios son similares a los que obtienen los ciudadanos (flexibilidad, ahorro de tiempo y dinero).

Gobierno a empleado (G2E). Son los portales encargados de satisfacer necesidades de información y servicios para los empleados de la administración pública.

Gobierno a gobierno (G2G). Responde a la gestión gubernamental proporcionando diferentes servicios: planificación, inventarios, adquisiciones, entre otros.[218]

Actualmente, uno de los nuevos retos o paradigmas que presentan las Tecnologías de la información es el desarrollo del cómputo en la nube o *Cloud Computing*; se trata de una forma novedosa en la prestación de los servicios de las TIC's a sus múltiples usuarios.

De acuerdo con Peter Mell y Timothy Grance, la computación en la nube o *cloud computing*, "es un modelo para habilitar el acceso de red ubicuo, conveniente y bajo demanda a una red compartida, conjunto de recursos informáticos configurables que se puede aprovisionar y liberar rápidamente con un mínimo esfuerzo de gestión o interacción con el proveedor de servicios"[219]; es decir, tener acceso a aplicaciones, datos, almacenamiento y servicios compartidos a través de una red, en el momento en que sea requerido y en el lugar donde sea requerido; todo ello, mediante una gran variedad de medios tecnológicos que el usuario puede emplear para acceder a dichos recursos, desde teléfonos inteligentes y tabletas, hasta notebooks y computadoras de escritorio, sin importar el sistema operativo que utilicen.

Por su parte, Google utiliza el término de *cloud computing* como: "La disponibilidad bajo demanda de recursos de computación como servicios a través de Internet. Esta tecnología evita que las empresas tengan que encargarse de aprovisionar, configurar o gestionar los recursos y permite que paguen únicamente por los que usen."[220]

En noviembre del 2015, la Unión internacional de Telecomunicaciones (UIT) [Organismo Dependiente de la ONU] aprobó la que sería la primera norma sobre la regulación de *big data*. Esta norma define al *big data* como: "Un paradigma para permitir la recopilación, el almacenamiento, la gestión, el análisis y la visualización,

---

[218] Pérez Zúñiga, Ricardo, *et. al. Análisis general del gobierno electrónico en México*, Revista de Tecnología y Sociedad [en línea] México, UDG, Año 5, número 9, septiembre 2015-febrero 2016, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *http://www.udgvirtual.udg.mx/paakat/index.php/paakat/article/view/253/376*

[219] Mell ,Peter, y Grance, Timothy, *The NIST definition of cloud computing,* [en línea] EUA, *National Institute of Standards and Technology (NIST)*, 2011 , [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf* p. 2.

[220] Google, *¿Qué es el cloud computing?*, [en línea] Google Cloud, s/d, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://cloud.google.com/learn/what-is-cloud-computing?hl=es*

potencialmente bajo restricciones de tiempo real, de conjuntos de datos extensos con características heterogéneas. Nota: Los ejemplos de características de conjuntos de datos incluyen alto volumen, alta velocidad, gran variedad, etc."[221]

Asimismo, indica que el ecosistema de *big data* describe un entorno, llamado ecosistema de big data a través de roles y sub-roles. También define las actividades necesarias para los roles que proporcionan y consumen servicios de big data, así como las relaciones entre roles.

El ecosistema de *big data* incluye los siguientes roles:

a. Proveedor de datos;
b. Proveedor de servicios de big data;
c. Cliente de servicio de big data.

La propia UIT menciona que los beneficios clave del big data basado en la computación en la nube son:

- Escalabilidad. Los macrodatos deben tener capacidades para almacenar y procesar grandes volúmenes de datos. Por lo tanto, la escalabilidad es muy importante para big data. Sin embargo, los sistemas adicionales para big data requieren mucho tiempo y gestión de costes. La computación en la nube puede proporcionar escalabilidades flexibles para big data sin una expansión adicional de la infraestructura. Permite al usuario del servicio de big data escalar o reducir fácilmente los recursos rápidamente.
- Resistencia. La computación en la nube puede admitir big data para tener capacidades de resiliencia para mantener un nivel de servicio aceptable frente a fallas que afecten el funcionamiento normal.
- Rentabilidad. Big Data facilita el procesamiento de datos rápido y escalable, como el análisis de registros del sistema y el análisis de flujos de clics. Para muchos sistemas y plataformas, existen grandes volúmenes de datos de registro y, tradicionalmente, las bases de datos se utilizan para realizar análisis de registros. Pero el costo de realizar análisis de datos (incluidos los costos de almacenamiento, mantenimiento del sistema, etc.) es demasiado alto cuando se utilizan mecanismos tradicionales. La computación en la nube puede ofrecer recursos flexibles y escalables de manera rentable.

[221] Unión Internacional de Telecomunicaciones, *Big Data – Cloud computing based requirements and capabilities*, UIT, noviembre 2015, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12584* p. 11.

- Análisis eficiente. Para extraer información más valiosa, las aplicaciones y servicios de big data necesitan una estrategia analítica bien definida, así como poder de procesamiento. El servicio de big data basado en la computación en la nube puede utilizar dinámicamente los recursos necesarios.
- Extracción de información profunda. Big Data desarrolla nuevos conocimientos y mecanismos comerciales, incluida la predicción y la asistencia para la toma de decisiones. Esto es diferente de los sistemas convencionales porque ya se conoce la lógica de procesamiento de datos para manejar los datos sin procesar y qué tipo de información se puede extraer de los conjuntos de datos.

Ahora bien, existe una relación entre la edad y el empleo de la tecnología, esto se ve reflejado en la forma en que las generaciones la usan. Los avances actuales en materia de tecnología han provocado que la separación entre las generaciones aumente de manera drástica.

El segmento de mayores de 50 años pertenece a los *baby boomers*, para quienes el uso de plataformas por internet, dispositivos digitales y comercio electrónico es significativamente menor en comparación con otros perfiles de edad, explicado por sus hábitos de consumo y menores habilidades digitales, como se aprecia en el siguiente cuadro:[222]

Concepto	*Baby Boomers* (1945-1964)	Generación X (1965-1989)	Millenials (1990-2000)	Generación Z (2001-Actualidad)
Penetración de *smartphone*	75.2%	89.4%	93.4%	95.8%
Gasto promedio por equipo	$2,773.0	$3,401.3	$3,626.8	$3,463.5
Gasto promedio en servicios móviles (ARPU)	$124.7	$141.5	$149.6	$109.5
Penetración de tabletas	11.7%	27.0%	28.6%	31.9%
Uso de Banda Ancha Móvil (BAM)	56.1%	66.9%	69.7%	68.8%
Comercio electrónico	58.5%	65.8%	79.6%	63.7%
Videojuegos	35.9%	51.1%	83.6%	85.0%

Fuente: The Competitive Intelligence Unit (The CIU), 2017

[222] Procuraduría Federal del Consumidor, *Tecnologías de la información y comunicación. Que la edad no sea un obstáculo*, [en línea], México, Profeco, 28 de agosto de 2019, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.gob.mx/profeco/documentos/tecnologias-de-la-informacion-y-comunicacion-que-la-edad-no-sea-un-obstaculo?state=published*

Imagen: Acceso y uso de las TIC en generaciones.
Tomada de: Procuraduría Federal del Consumidor, *Tecnologías de la información y comunicación. Que la edad no sea un obstáculo*, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.gob.mx/profeco/documentos/tecnologias-de-la-informacion-y-comunicacion-que-la-edad-no-sea-un-obstaculo?state=published*

Ya para terminar este punto, vale la pena mencionar que, de acuerdo con datos del INEGI, de acuerdo con la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2020[223], en México, se estimó una población de 84.1 millones de usuarios de internet, que representan 72.0% de la población de seis años o más. Esta cifra revela un aumento de 1.9 puntos porcentuales respecto a la registrada en 2019 (70.1%).

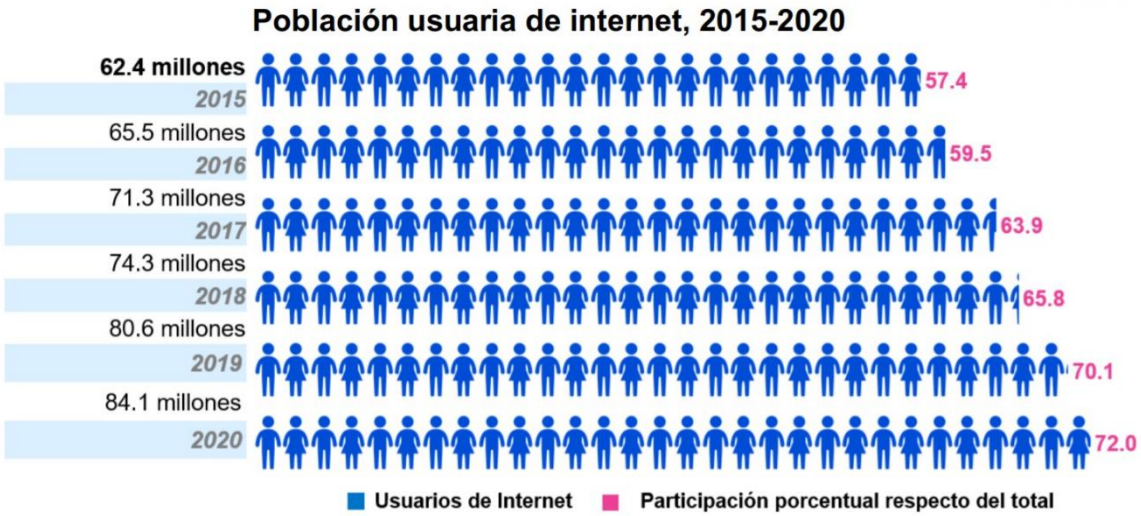


Imagen: Población usuaria de internet, 2015-2020.
Tomada de: Instituto Nacional de Estadística y Geografía, *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2020*, [en línea] México, INEGI-IFT, 2020, *http://www.ift.org.mx/sites/default/files/comunicacion-y-medios/comunicados-ift/comunicadoendutih2020.pdf*

Según datos de la encuesta, se estima, que de los 84.1 millones de usuarios de internet de seis años o más captados por la ENDUTIH 2020, son usuarios 71.3% de las mujeres y 72.7% de los hombres, esto respecto de la distribución poblacional por sexo.

[223] Instituto Nacional de Estadística y Geografía, *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2020*, [en línea] México, INEGI-IFT, 2020, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *http://www.ift.org.mx/sites/default/files/comunicacion-y-medios/comunicados-ift/comunicadoendutih2020.pdf* p. 1.

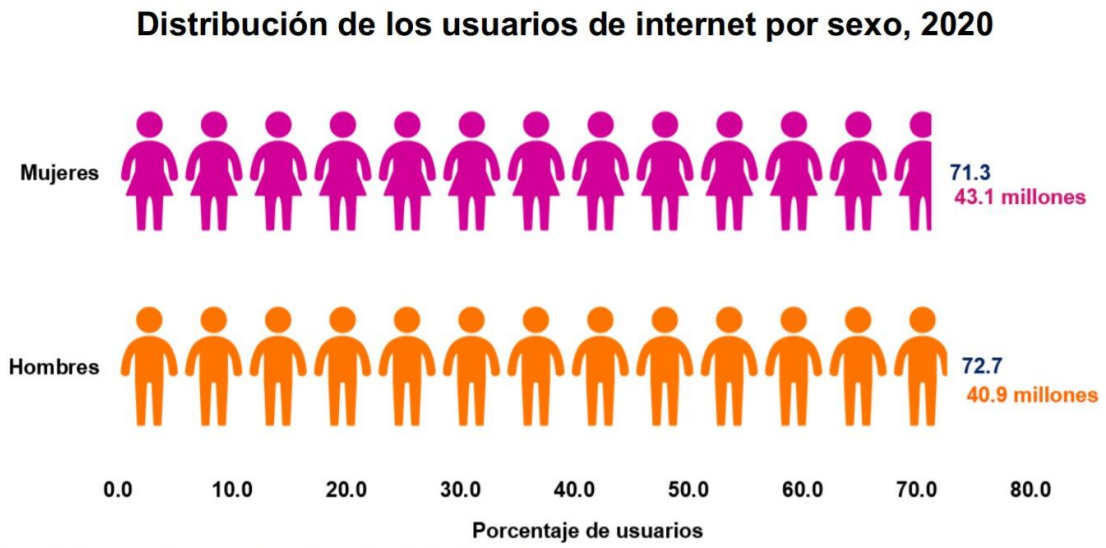


Imagen: Distribución de los usuarios de internet por sexo, 2020.

Tomada de: Instituto Nacional de Estadística y Geografía, *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2020*, [en línea] México, INEGI-IFT, 2020, *http://www.ift.org.mx/sites/default/files/comunicacion-y-medios/comunicados-ift/comunicadoendutih2020.pdf*

Asimismo, analizando el comportamiento de los distintos grupos de edad de la población total, el que concentra la mayor proporción de usuarios de internet respecto al total de cada grupo de edad, es el grupo de 18 a 24 años con una participación de 90.5%. El segundo grupo de edad donde el uso de internet está más generalizado, es el de 12 a 17 años, con 90.2%. En tercer lugar, se encuentran los usuarios de 25 a 34 años, quienes registraron 87.1%. Por su parte, el grupo de edad que menos usa internet es el de 55 y más años, ya que registraron 37.5 por ciento.

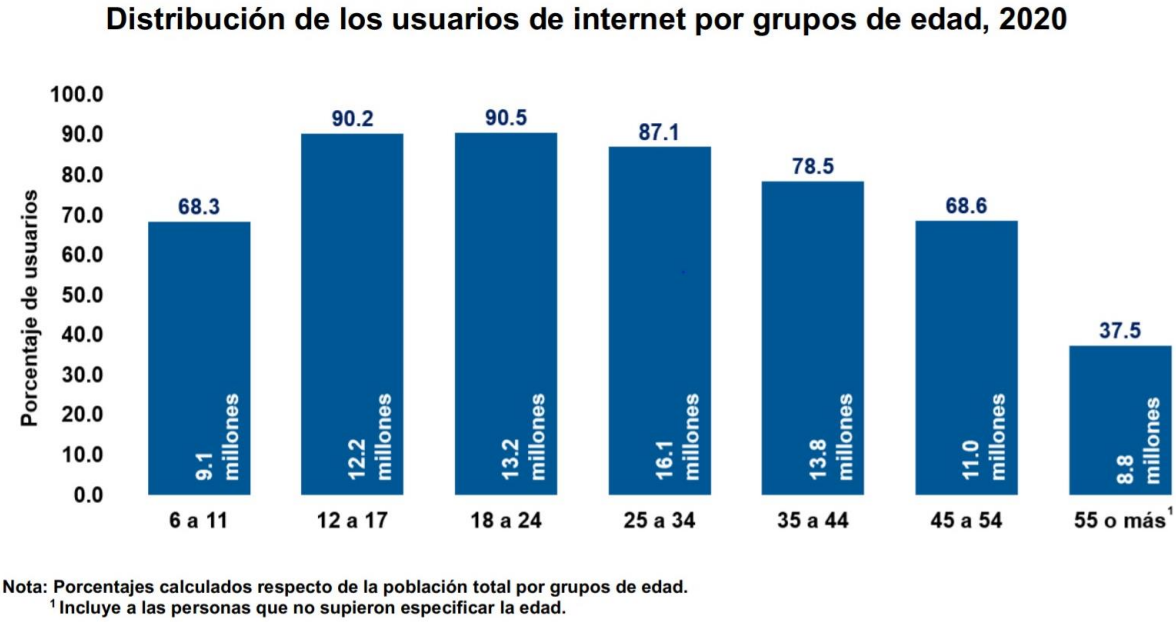


Imagen: Distribución de los usuarios de internet por grupos de edad, 2020.

Tomada de: Instituto Nacional de Estadística y Geografía, *Encuesta Nacional sobre Disponibilidad y Uso de*

Tecnologías de la Información en los Hogares (ENDUTIH) 2020, [en línea] México, INEGI-IFT, 2020, *http://www.ift.org.mx/sites/default/files/comunicacion-y-medios/comunicados-ift/comunicadoendutih2020.pdf*

2.5. Riesgos del uso del *Big Data*

Los elementos fundamentales de los derechos humanos deben protegerse para poder aprovechar las oportunidades que ofrecen los macrodatos. El derecho a la intimidad, la ética y el respeto requieren que evaluemos los derechos de los individuos con los beneficios de lo colectivo. Gran parte de los nuevos datos se recoge de manera pasiva a través de la «huella digital» que dejan las personas en los sensores que tienen los distintos dispositivos y aplicaciones o a través de algoritmos. La combinación de todos estos datos puede llevar a la identificación de individuos o grupos de individuos, haciéndolos susceptibles a una posible amenaza. Deben ponerse en práctica medidas apropiadas para la protección de los datos y evitar su mala gestión o uso incorrecto.

Existe también un riesgo de aumento de la desigualdad. Ya están surgiendo grandes diferencias entre aquellos que tienen acceso a la información y los que no. Si no se adoptan medidas, una frontera de desigualdad totalmente nueva dividirá el mundo entre aquellos que saben y los que no. Muchas personas están excluidas del nuevo mundo de los datos y la información a causa del idioma, la pobreza, la falta de educación, la falta de infraestructuras tecnológicas, el aislamiento o el prejuicio y la discriminación. Hay un amplio espectro de acciones necesarias entre las que se incluyen el desarrollo de las capacidades de todos los países y en particular los Países Menos Adelantados (PMA), los Países en Desarrollo sin Litoral (PDSL) y los Pequeños Estados Insulares en Desarrollo (PEID).[224]
La ONU ha tenido en cuenta también diferentes riesgos en el manejo de los macrodatos: “existen preocupaciones legítimas sobre riesgos asociados con el manejo y procesamiento de macrodatos, particularmente a la luz de la actual fragmentación regulatoria y en ausencia de un conjunto común de principios sobre privacidad, ética y protección de datos. Estas preocupaciones continúan complicando los esfuerzos para desarrollar y enfoques escalables para la gestión de riesgos y los datos acceso. Se requiere un enfoque coordinado para garantizar la aparición de marcos para el uso seguro y responsable de *big data* para la consecución de la Agenda 2030.”[225]

Los principios de esta guía son los siguientes:

1. Uso legal, legítimo y justo.
2. Especificación de Propósitos. Uso, limitación y finalidad de compatibilidad.

[224] Organización de las Naciones Unidas, *Macrodatos para el desarrollo sostenible*, [en línea]ONU, sección Desafíos Globales, 2018, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.un.org/es/global-issues/big-data-for-sustainable-development*
[225] Organización de las Naciones Unidas, *Data Privacy, Ethics and Protection. Guidance note on Big Data for Achievement of the 2030 Agenda*, ONU Development Group, 2017, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://unsdg.un.org/es/resources/confidencialidad-etica-y-proteccion-de-datos-nota-orientativa-sobre-macrodatos-big-data* p. 2.

3. Mitigación de Riesgos y Evaluación de Riesgos, Daños y Beneficios.
4. Datos sensibles, y contextos sensibles.
5. Seguridad de Datos.
6. Retención y minimización de datos.
7. Calidad de Datos.
8. Datos Abiertos, Transparencia y Responsabilidad «Accountability» [o Rendición de Cuentas]
9. Debida Diligencia para terceros Colaboradores.

Es importante mencionar que en la norma de la UIT las tecnologías y servicios de *big data* permiten resolver muchos desafíos nuevos y también crean más oportunidades nuevas que nunca:

- Heterogeneidad e incompletitud: los datos procesados mediante big data pueden perder algunos atributos o introducir ruido en la transmisión de datos. Incluso después de la limpieza de datos y la corrección de errores, es probable que persistan algunos datos incompletos y algunos errores. Estos desafíos se pueden gestionar durante el análisis de datos. [b-CRA-BDWP]
- Escala: el procesamiento de grandes volúmenes de datos que crecen rápidamente es una tarea desafiante. Al utilizar tecnologías de procesamiento de datos, el desafío de la escala de datos se mitigó con la evolución de los recursos de procesamiento y almacenamiento. Sin embargo, hoy en día los volúmenes de datos están escalando más rápido de lo que pueden evolucionar los recursos. Tecnologías como bases de datos paralelas, bases de datos en memoria, bases de datos no SQL y algoritmos analíticos permiten resolver este desafío.

- Puntualidad: la tasa de adquisición y la puntualidad, para encontrar de manera efectiva elementos en un tiempo limitado que cumplan con un criterio específico en un gran conjunto de datos, son nuevos desafíos a los que se enfrenta el procesamiento de datos. Otros nuevos desafíos están relacionados con los tipos de criterios especificados y existe la necesidad de diseñar nuevas estructuras de índices y respuestas a las consultas con límites de tiempo de respuesta ajustados.

- Privacidad: Los datos sobre personas humanas, como información demográfica, actividades en Internet, patrones de conmutación, interacciones sociales, consumo de energía o agua, se recopilan y analizan para diferentes propósitos. Las tecnologías y servicios de big data tienen el desafío de proteger las identidades personales y los atributos confidenciales de los datos a lo largo de todo el ciclo de procesamiento de datos, respetando la política de retención de datos aplicable.[226]

La resolución positiva de los desafíos anteriores abre nuevas oportunidades para descubrir nuevas relaciones de datos, patrones ocultos o dependencias desconocidas.

[226] Unión Internacional de Telecomunicaciones, *Big Data*, *op cit.* p. 4.

Capítulo 3. Régimen Jurídico de la Transparencia y Acceso a la Información Pública Gubernamental

3.1. Aspectos Generales

Se dice que la transparencia es un asunto de dos:[227]

1) El interesado que tienen derecho a saber y a preguntar sobre lo que hace el gobierno.
2) El sujeto obligado que tiene la obligación de informar sobre lo que hace.

Es un asunto de dos porque:

1) Si la población no pregunta, no pide cuentas, no se interesa en saber lo que hace el gobierno, la transparencia no es posible.
2) Si los sujetos obligados se niegan a proporcionar información pública a la población y a rendir cuentas sobre su quehacer, la transparencia tampoco se da.

Para que la transparencia sea posible, se requiere de sujetos obligados abiertos de cara a la sociedad, de una sociedad interesada y participante en el quehacer público.[228]
Esquemáticamente sería de la siguiente forma:

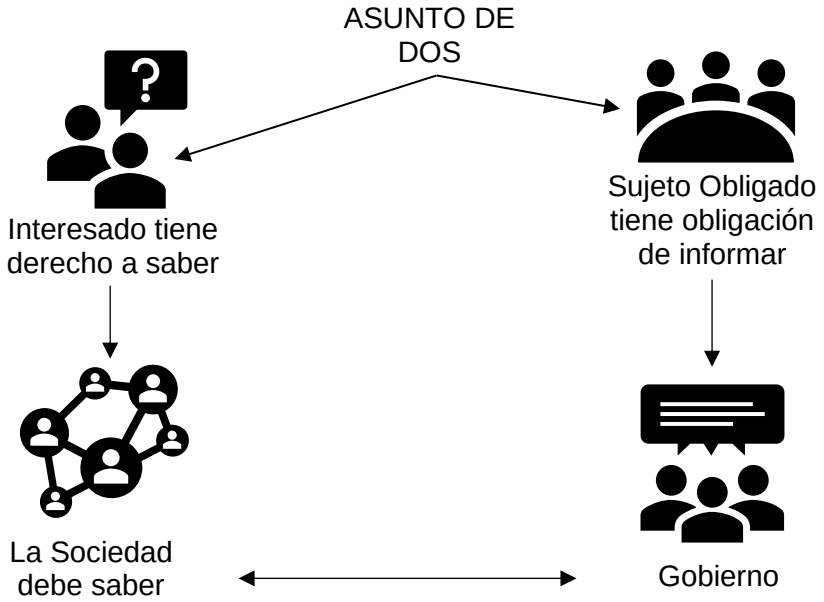


Imagen: Transparencia, un asunto de dos.
Tomada de: Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, *La Transparencia: Un asunto de Dos*, [en línea] México, InfoDF, 2009, [fecha de consulta: 3 de diciembre de 2022] Disponible en:
http://www.infodf.org.mx/capacitacion/publicacionesDCCT/Unasuntodedos/unasuntodedos.pdf p. 5.

[227] Adaptado de Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, *La Transparencia: Un asunto de Dos*, [en línea] México, InfoDF, 2009, [fecha de consulta: 3 de diciembre de 2022] Disponible en:
http://www.infodf.org.mx/capacitacion/publicacionesDCCT/Unasuntodedos/unasuntodedos.pdf p. 5.
[228] *Ídem*.

En ese tenor, información pública es el conjunto de datos de autoridades o particulares en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, obtenidos por causa del ejercicio de funciones de derecho público, considerando que en este ámbito de actuación rige la obligación de éstos de rendir cuentas y transparentar sus acciones frente a la sociedad.[229]

El pleno de la Suprema Corte de Justicia de la Nación ha indicado que el acceso a la información se distingue de otros derechos intangibles por su doble carácter: como un derecho en sí mismo y como un medio o instrumento para el ejercicio de otros derechos. A continuación, se expone la siguiente tesis de Jurisprudencia:

> **ACCESO A LA INFORMACIÓN. SU NATURALEZA COMO GARANTÍAS INDIVIDUAL Y SOCIAL.**
> El acceso a la información se distingue de otros derechos intangibles por su doble carácter: **como un derecho en sí mismo y como un medio o instrumento para el ejercicio de otros derechos**. En efecto, además de un valor propio**, la información tiene uno instrumental que sirve como presupuesto del ejercicio de otros derechos y como base para que los gobernados ejerzan un control respecto del funcionamiento institucional de los poderes públicos, por lo que se perfila como un límite a la exclusividad estatal en el manejo de la información y, por ende, como una exigencia social de todo Estado de Derecho.** Así, el acceso a la información como garantía individual **tiene por objeto maximizar el campo de la autonomía personal, posibilitando el ejercicio de la libertad de expresión en un contexto de mayor diversidad de datos, voces y opiniones**; incluso **algunos instrumentos internacionales lo asocian a la libertad de pensamiento y expresión**, a las cuales describen como el derecho que comprende la libertad de **buscar**, **recibir** y **difundir** informaciones e ideas de toda índole. Por otro lado, el acceso a la información como derecho colectivo o garantía social cobra un marcado carácter público en tanto que funcionalmente tiende a revelar el empleo instrumental de la información no sólo como factor de autorrealización personal, sino como **mecanismo de control institucional**, pues se trata de un derecho fundado en una de las características principales del gobierno republicano, que es el de la publicidad de los actos de gobierno y la transparencia de la administración. Por tanto, este derecho resulta ser una consecuencia directa del principio administrativo de transparencia de la información pública gubernamental y, a la vez, se vincula con el derecho de participación de los ciudadanos en la vida pública, protegido por la Constitución Política de los Estados Unidos Mexicanos.[230]

[229] INFORMACIÓN PÚBLICA. ES AQUELLA QUE SE ENCUENTRA EN POSESIÓN DE CUALQUIER AUTORIDAD, ENTIDAD, ÓRGANO Y ORGANISMO FEDERAL, ESTATAL Y MUNICIPAL, SIEMPRE QUE SE HAYA OBTENIDO POR CAUSA DEL EJERCICIO DE FUNCIONES DE DERECHO PÚBLICO. Tesis: 2a. LXXXVIII/2010, Semanario Judicial de la Federación y su Gaceta Registro, Novena Época, t. XXXII, agosto de 2010, p. 463.

[230] Tesis P./J. 54/2008, Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XXVII, junio de 2008, p. 743.

La libertad de expresión y el derecho a la información son derechos funcionalmente centrales en un estado constitucional y tienen una doble faceta: por un lado, aseguran a las personas espacios esenciales para el despliegue de su autonomía y, por otro, gozan de una vertiente pública, colectiva o institucional que los convierte en piezas básicas para el adecuado funcionamiento de la democracia representativa.

Así, tener plena libertad para expresar, recolectar, difundir y publicar informaciones e ideas es imprescindible no solamente como instancia esencial de autoexpresión y desarrollo individual, sino como condición para ejercer plenamente otros derechos fundamentales -el de asociarse y reunirse pacíficamente con cualquier objeto lícito, el derecho de petición o el derecho a votar y ser votado- y como elemento determinante de la calidad de la vida democrática en un país, pues si los ciudadanos no tienen plena seguridad de que el derecho los protege en su posibilidad de expresar y publicar libremente ideas y hechos, será imposible avanzar en la obtención de un cuerpo extenso de ciudadanos activos, críticos, comprometidos con los asuntos públicos, atentos al comportamiento y a las decisiones de los gobernantes, capaces de cumplir la función que les corresponde en un régimen democrático.[231]

Adicionalmente, resulta interesante adicionar que las normas penales no pueden restringir el goce del núcleo esencial del derecho a la información. La mera existencia de una norma que penalice *ab initio* la búsqueda de información y que, además, se considere *prima facie* y sin una declaratoria previa de clasificada o reservada y sin que supere una prueba de daño, puede constituir un efecto amedrentador (*chilling effect*) en un periodista, puesto que, al margen de que se llegue o no a comprobar su responsabilidad, el simple hecho de ser sometido a un proceso penal puede fácilmente disuadirlo de cumplir con su labor profesional, ante la amenaza real de ser sometido a uno o varios procesos de carácter penal. De manera que puede existir una afectación por el simple hecho de someter a un periodista a un proceso penal como consecuencia del ejercicio legítimo del derecho de acceso a la información y puede, además, llevar a un uso desproporcionado del derecho penal. En consecuencia, las normas penales no pueden restringir el goce del núcleo esencial del derecho de acceso a la información, ni criminalizar la discusión pública de un fragmento de la actividad del poder público que, idealmente, se debería ubicar en el centro de la evaluación de la sociedad, como lo es lo relativo a la seguridad pública, y que no se limita a restringir aspectos incidentales o periféricos al discurso.[232]

Asimismo, ese derecho del individuo, con la adición al contenido original del artículo

[231] LIBERTAD DE EXPRESIÓN Y DERECHO A LA INFORMACIÓN. SU IMPORTANCIA EN UNA DEMOCRACIA CONSTITUCIONAL. Tesis 1a. CCXV/2009, Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XXX, diciembre de 2009, p. 287.
[232] ACCESO A LA INFORMACIÓN. LAS NORMAS PENALES NO PUEDEN RESTRINGIR EL GOCE DEL NÚCLEO ESENCIAL DE ESTE DERECHO. Tesis: 1a. CCCXCIX/2015 (10a.) Gaceta del Semanario Judicial de la Federación, Décima Época, t. I, diciembre de 2015, p. 253.

6o., quedó también equilibrado con el derecho que tiene la sociedad a estar veraz y objetivamente informada, para evitar que haya manipulación. Así, el Estado asume la obligación de cuidar que la información que llega a la sociedad a través de los grandes medios masivos de comunicación, refleje la realidad y tenga un contenido que permita y coadyuve al acceso a la cultura en general, para que el pueblo pueda recibir en forma fácil y rápida conocimientos en el arte, la literatura, en las ciencias y en la política. Ello permitirá una participación informada para la solución de los grandes problemas nacionales, y evitará que se deforme el contenido de los hechos que pueden incidir en la formación de opinión.

Luego, en el contenido actual del artículo 6o., se consagra la libertad de expresarse, la cual es consustancial al hombre, y que impide al Estado imponer sanciones por el solo hecho de expresar las ideas. Pero correlativamente, esa opinión tiene límites de cuya transgresión derivan consecuencias jurídicas. Tales límites son que la opinión no debe atacar la moral, esto es, las ideas que se exterioricen no deben tender a destruir el conjunto de valores que sustenta la cohesión de la sociedad en el respeto mutuo y en el cumplimiento de los deberes que tienen por base la dignidad humana y los derechos de la persona; tampoco debe dañar los derechos de tercero, ni incitar a la provocación de un delito o a la perturbación del orden público.[233]

Otros derechos que pueden ser ejercidos en aras de la Transparencia son los de:

1) Rendición de cuentas,
2) Datos Personales, (Derechos ARCO o ARCOP)
3) Consultas públicas,
4) Derechos de conocer la interconexión e interoperabilidad de las redes públicas de telecomunicaciones concesionadas,
5) Solicitud de un expediente clínico.

En el caso de pueblos y comunidades indígenas, se deben cubrir ciertos requisitos esenciales para dar cabal cumplimiento en su derecho a ser consultados. De conformidad con los estándares internacionales en materia de protección a los derechos de las comunidades indígenas, las características específicas del procedimiento de consulta variarán necesariamente en función de la naturaleza de la medida propuesta y del impacto sobre los grupos indígenas.[234]

[233] DERECHO A LA INFORMACIÓN. NO DEBE REBASAR LOS LÍMITES PREVISTOS POR LOS ARTÍCULOS 6o., 7o. Y 24 CONSTITUCIONALES. Tesis: I.3o.C.244 C, Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XIV, septiembre de 2001, p. 1309.
[234] PUEBLOS Y COMUNIDADES INDÍGENAS. DERECHO A SER CONSULTADOS. REQUISITOS ESENCIALES PARA SU CUMPLIMIENTO. Tesis: 2a. XXIX/2016 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. II, junio de 2016, p. 1212.

Imagen: Requisitos esenciales para el cumplimiento al derecho de consulta de pueblos y comunidades indígenas.
Fuente: Elaboración propia, tomada a partir de: PUEBLOS Y COMUNIDADES INDÍGENAS. DERECHO A SER CONSULTADOS. REQUISITOS ESENCIALES PARA SU CUMPLIMIENTO. Tesis: 2a. XXIX/2016 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. II, junio de 2016, p. 1212.

Ahora bien, existen materias de carácter transversal como competencia económica, radiodifusión y telecomunicaciones donde se involucra, en ciertos casos, a autoridades distintas del Instituto Federal de Telecomunicaciones y de la Comisión Federal de Competencia Económica; y dado el carácter transversal de esas materias en aspectos como: derechos humanos, rectoría económica, libre concurrencia y regulación, como es, entre otros, el derecho de acceso a la información. Un supuesto de esos conceptos comunes es la transparencia que, como garantía institucional, comparte esa transversalidad y dimensión objetiva de los derechos fundamentales y, por tanto, debe ser aplicada por todas las autoridades en las distintas circunstancias que lo ameriten.

Así, el marco jurídico aplicable a los servicios de telecomunicaciones se complementa con reconocer y observar principios como la transparencia y, en el caso concreto, respecto de los términos y condiciones pertinentes para regular y promover la eficiente interconexión e interoperabilidad de las redes públicas de telecomunicaciones concesionadas.[235]

[235] PLAN TÉCNICO FUNDAMENTAL DE INTERCONEXIÓN E INTEROPERABILIDAD, PUBLICADO EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 10 DE FEBRERO DE 2009. SUS ARTÍCULOS 3, 5, 8, 10, 15, 24, 28 Y 34, NO VIOLAN EL PRINCIPIO DE DISTRIBUCIÓN DE COMPETENCIAS ESPECIALIZADAS EN LA ADMINISTRACIÓN PÚBLICA FEDERAL, NI

Por su parte, los derechos de acceso a la información y a la salud guardan una relación de interdependencia cuando, en ejercicio del primero, se solicita copia certificada de un expediente clínico. Por tanto, la autoridad que se pronuncie en relación con el costo de la expedición de la copia certificada del expediente clínico del solicitante, debe observar el principio *pro-persona*.[236]

Para finalizar este apartado, cabe señalar que el pasado 17 de junio de 2015 se publicó en el Diario Oficial de la Federación (DOF), el acuerdo mediante el cual el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, establece las bases de interpretación y aplicación de la Ley General de Transparencia y Acceso a la Información Pública. Dicho acuerdo tiene como objeto brindar certeza, objetividad, legalidad y seguridad jurídica a todas las personas y a las autoridades, entidades, órganos y organismos de los Poderes Ejecutivos, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, respecto del alcance y aplicación de la Ley General de Transparencia y Acceso a la Información Pública.

3.1.1. Principios Rectores

Las leyes modernas administrativas en México, están plagadas de principios como parte de los componentes que se deben observar dentro de un sistema normativo. En este sentido, la función de un sistema normativo consiste en establecer correlaciones deductivas entre reglas, casos y soluciones, y esto quiere decir que, del conjunto formado por el sistema normativo y un enunciado descriptivo de un caso, se deduce una respuesta o solución. Por su parte, dentro de las propiedades estructurales de los sistemas normativos, se encuentran la completitud, la independencia y la coherencia. En suma, un sistema normativo es un conjunto de **reglas, valores y principios**, coherentes entre sí, que interactúan y rigen determinados supuestos, por lo que el alcance de cada uno depende del otro, con las propiedades de completitud, independencia y coherencia.[237]

De conformidad con el decreto publicado en el Diario Oficial de la Federación el seis de diciembre de mil novecientos setenta y siete, el constituyente permanente

---

PROVOCAN UNA DOBLE REGULACIÓN EN MATERIA DE ACCESO A LA INFORMACIÓN. Tesis: I.1o.A.E.135 A (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. IV, mayo de 2016, p. 2830.

[236] COPIA CERTIFICADA DE UN EXPEDIENTE CLÍNICO. CUANDO SE SOLICITA EN EJERCICIO DEL DERECHO DE ACCESO A LA INFORMACIÓN, LA AUTORIDAD QUE SE PRONUNCIE EN RELACIÓN CON EL COSTO DE SU EXPEDICIÓN, EN OBSERVANCIA AL PRINCIPIO PRO PERSONA, NO DEBE APLICAR EL ARTÍCULO 83, FRACCIÓN I, DE LA LEY DE INGRESOS DEL ESTADO DE PUEBLA, PARA EL EJERCICIO FISCAL 2015, QUE PREVÉ LA CUOTA APLICABLE POR LA CERTIFICACIÓN DE DATOS O DOCUMENTOS. Tesis: VI.2o.A.11 A (10a.) Gaceta del Semanario Judicial de la Federación, t. IV, octubre de 2016, p. 2852.

[237] SISTEMA NORMATIVO. CONCEPTO Y FUNCIÓN. Tesis: I.4o.A.43 K (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. II, marzo de 2020, p. 1027.

reformó el artículo 6o. constitucional, a efecto de actualizar el concepto tradicional que se tenía de la libertad de expresión, pues la doctrina moderna considera que tal prerrogativa constituye una de las piedras angulares de las democracias contemporáneas y que tiene dos vertientes: por un lado el derecho a informar y emitir mensajes, y por otro, el derecho a ser informado, por lo que fue este último aspecto el que fue instituido con la citada reforma al establecerse que el derecho a la información será garantizado por el Estado.

Esta importante adición encuentra sustento en el principio de la publicidad de los actos de gobierno, conforme al cual la información constituye un factor de control del ejercicio del poder público, dado que los diversos entes estatales se encuentran obligados a dar a conocer cada uno de sus actos públicos, que sean de interés general, para transparentar el debido cumplimiento de las funciones que tengan encomendadas, salvo los datos que sean catalogados como confidenciales; no obstante, el desarrollo del derecho de acceso a la información se ha enfrentado a diversas problemáticas, resistencias y deformaciones, principalmente por la heterogeneidad con la que se legisló sobre el particular en las distintas entidades federativas de la República, provocando una diversidad perjudicial para su consolidación, ante la falta de una "guía constitucional".[238]

De conformidad con el texto del artículo 6o. constitucional, el derecho a la

[238] DERECHO A LA INFORMACIÓN PÚBLICA. EVOLUCIÓN CONSTITUCIONAL DE LA REGULACIÓN DE ESA PRERROGATIVA. Tesis: I.15o.A.118 A, Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XXIX, abril de 2009, p. 1880.

información comprende las siguientes garantías:[239]

Imagen: Garantías del derecho a la información.
Fuente: Elaboración propia a partir de tesis: 2a. LXXXV/2016 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. I, septiembre de 2016, p. 839.

No obstante, el principal principio relacionado con el acceso a la información es el llamado principio de máxima publicidad. La Constitución Política de los Estados Unidos Mexicanos lo nombra de la siguiente manera: “En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad.”

Del artículo 6o. de la CPEUM se advierte que el Estado Mexicano está constreñido a publicitar sus actos, pues se reconoce el derecho fundamental de los ciudadanos a acceder a la información que obra en poder de la autoridad. Por ello, el principio de máxima publicidad incorporado en el texto constitucional, implica para cualquier autoridad, realizar un manejo de la información bajo la premisa inicial que toda ella es pública y sólo por excepción, en los casos expresamente previstos en la legislación secundaria y justificados bajo determinadas circunstancias, se podrá clasificar como confidencial o reservada, esto es, considerarla con una calidad diversa.[240]

Asimismo, el derecho a la información consagrado en la última parte del artículo 6o. de la constitución federal no es absoluto; sino que, como toda garantía, se halla sujeto a limitaciones o excepciones que se sustentan, fundamentalmente, en la protección de la seguridad nacional y en el respeto tanto a los intereses de la sociedad como a los derechos de los gobernados, limitaciones que, incluso, han dado origen a la figura jurídica del secreto de información que se conoce en la doctrina como "reserva de información" o "secreto burocrático". En este sentido, el respeto a su ejercicio encuentra excepciones que lo regulan y a su vez lo garantizan, en atención a la materia a que se refiera; así, en cuanto a la seguridad nacional, se tienen normas que, por un lado, restringen el acceso a la información en esta materia, en razón de que su conocimiento público puede generar daños a los intereses nacionales y, por el otro, sancionan la inobservancia de esa reserva; por lo que hace al interés social, se cuenta con normas que tienden a proteger la averiguación de los delitos, la salud y la moral públicas, mientras que por lo que respecta a la protección de la persona existen normas que protegen el derecho a la vida o a la privacidad de los gobernados.[241]

Si bien es cierto que el artículo 6o. de la Constitución Política de los Estados Unidos

[239] DERECHO A LA INFORMACIÓN. GARANTÍAS DEL. Tesis: 2a. LXXXV/2016 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. I, septiembre de 2016, p. 839.
[240] ACCESO A LA INFORMACIÓN. IMPLICACIÓN DEL PRINCIPIO DE MÁXIMA PUBLICIDAD EN EL DERECHO FUNDAMENTAL RELATIVO. Tesis: I.4o.A.40 A (10a.), Semanario Judicial de la Federación y su Gaceta, Décima Época, t. III, marzo de 2013, p. 1899.
[241] DERECHO A LA INFORMACIÓN. SU EJERCICIO SE ENCUENTRA LIMITADO TANTO POR LOS INTERESES NACIONALES Y DE LA SOCIEDAD, COMO POR LOS DERECHOS DE TERCEROS. Tesis: P. LX/2000, Semanario Judicial de la Federación y su Gaceta, t. XI, abril de 2000, p. 74.

Mexicanos establece los principios, directrices y reglas básicas sobre las cuales se construyen los sistemas de protección de datos personales y de transparencia y acceso a la información pública, también lo es que en el propio texto constitucional se contienen otras reglas específicas al respecto, como ocurre tratándose de la identidad y de los datos personales de las víctimas y ofendidos partes en el procedimiento penal (artículo 20, apartado C, fracción V), del régimen de telecomunicaciones (artículos tercero y octavo transitorios del decreto de reforma en la materia, publicado en el Diario Oficial de la Federación el 11 de junio de 2013), la fiscalización de recursos públicos ejercidos por personas privadas (artículo 79), la creación del Sistema Nacional de Información Estadística y Geográfica (artículo 26, apartado B), el registro público sobre deuda pública (artículo 73, fracción VIII, inciso 3o.), la investigación y sanción de responsabilidades administrativas y hechos de corrupción, tratándose de información fiscal o relacionada con el manejo de recursos monetarios (artículo 109, fracción IV), el Sistema de Información y Gestión Educativa (artículo quinto transitorio del decreto de reformas publicado en el señalado medio el 26 de febrero de 2013), la recopilación de información geológica y operativa a cargo de la Comisión Nacional de Hidrocarburos [artículo décimo transitorio, inciso b), del decreto de reformas constitucionales difundido el 20 de diciembre de 2013], el sistema de fiscalización sobre el origen y destino de los recursos de los partidos políticos, coaliciones y candidatos (artículo segundo transitorio del decreto de reformas publicado el 10 de febrero de 2014) y la fiscalización de la deuda pública (artículo séptimo transitorio del decreto que modifica diversas disposiciones constitucionales, publicado el 26 de mayo de 2015).[242]

Asimismo, de la declaración conjunta adoptada el 6 de diciembre de 2004 por el relator especial de las Naciones Unidas para la libertad de opinión y expresión, el representante de la Organización para la Seguridad y Cooperación en Europa para la Libertad de los Medios de Comunicación y el relator especial de la Organización de los Estados Americanos para la libertad de expresión, aplicable a la materia en virtud de lo dispuesto en el artículo 6 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, se advierten como principios básicos que rigen el acceso a la información los siguientes:

1) El derecho de acceso a ésta es un derecho humano fundamental;

2) El proceso para acceder a la información pública deberá ser simple, rápido y gratuito o de bajo costo; y,

3) Deberá estar sujeto a un sistema restringido de excepciones, las que sólo se aplicarán cuando exista el riesgo de daño sustancial a los intereses protegidos y cuando ese daño sea mayor que el interés público en

[242] SISTEMAS DE PROTECCIÓN DE DATOS PERSONALES Y DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. PRECEPTOS CONSTITUCIONALES QUE LOS REGULAN. Tesis: I.2o.A.E.1 CS (10a.), Décima Época, Gaceta del Semanario Judicial de la Federación, t. III, febrero de 2017, p. 2364.

general de tener acceso a la información.[243]

Finalmente, y atento a la importancia de las nuevas tecnologías de la información y la comunicación que permiten la existencia de una red mundial en la que pueden intercambiarse ideas y opiniones, conforme a lo sostenido por el Comité de Derechos Humanos de la Organización de las Naciones Unidas, el Estado debe tomar todas las medidas necesarias para fomentar la independencia de esos nuevos medios y asegurar a los particulares el acceso a éstos, pues precisamente el intercambio instantáneo de información e ideas a bajo costo, a través del Internet, facilita el acceso a información y conocimientos que antes no podían obtenerse lo cual, a su vez, contribuye al descubrimiento de la verdad y al progreso de la sociedad en su conjunto, a lo que se debe que el marco del derecho internacional de los derechos humanos siga siendo pertinente y aplicable a las nuevas tecnologías de la comunicación; de hecho, puede afirmarse que el Internet ha pasado a ser un medio fundamental para que las personas ejerzan su derecho a la libertad de opinión y de expresión, atento a sus características singulares, como su velocidad, alcance mundial y relativo anonimato. Por tanto, en atención a ese derecho humano, se reconoce que en el orden jurídico nacional y en el derecho internacional de los derechos humanos, existe el principio relativo a que el flujo de información por Internet debe restringirse lo mínimo posible, esto es, en circunstancias excepcionales y limitadas, previstas en la ley, para proteger otros derechos humanos.[244]

3.2. Sujetos Obligados

A juicio del que esto escribe, los Sujetos Obligados en materia de transparencia son aquellos que deben informar sobre sus acciones y justificarlas en público, conforme a la normatividad aplicable, estos sujetos son responsables ante quienes se vean afectados por sus decisiones, por lo que están obligados a rendir cuentas.

Hay que recordar que la evolución en cuanto al alcance de los sujetos obligados ha ido variando conforme a las modificaciones tanto al artículo 6° constitucional, como a las leyes en materia de transparencia, tanto por la hoy abrogada Ley Federal de Transparencia, como por la actual Ley General de Transparencia.

De hecho, vale mencionar que antes de la reforma constitucional del artículo 6° hubo alguna interpretación que consideraba lo siguiente:

El artículo 12 de la Ley de Transparencia e Información Pública del

[243] TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL. PRINCIPIOS FUNDAMENTALES QUE RIGEN ESE DERECHO. Tesis: I.8o.A.131 A, Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XXVI, octubre de 2007, p. 3345.
[244] FLUJO DE INFORMACIÓN EN RED ELECTRÓNICA (INTERNET). PRINCIPIO DE RESTRICCIÓN MÍNIMA POSIBLE. Tesis: 2a. CII/2017 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. II, junio de 2017, p. 1433.

> Estado de Jalisco, al contemplar como "sujetos obligados" a organismos ciudadanos, instituciones privadas y organismos no gubernamentales que reciban, administren o apliquen recursos públicos, contraviene el artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, porque al disponer éste que las leyes determinarán la manera en que los "sujetos obligados" deberán hacer pública la información relativa a los recursos públicos que entreguen a personas físicas o morales, distingue entre éstas y aquéllos, en el sentido de que los primeros son los que deben hacer pública la información de los recursos aplicados a los segundos, pues considerar lo contrario, como lo hace el precepto inicialmente citado, implicaría que cualquier gobernado puede acudir ante tales organismos e instituciones a exigir su derecho a la información, lo que resultaría un contrasentido y derivaría en un conflicto entre particulares.[245]

Para entender lo anterior, será necesario tener una comparativa entre los sujetos obligados:

DOF: 20/07/2007 Se adiciona un segundo párrafo con siete fracciones al Artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, para quedar como sigue:	DOF: 07/02/2014 DECRETO por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia.
Artículo 6o.- ... 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: I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes. En la interpretación de este	Artículo 6o. ... ... A. 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: I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos,

[245] TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. EL ARTÍCULO 12 DE LA LEY RELATIVA DEL ESTADO DE JALISCO, AL CONTEMPLAR COMO "SUJETOS OBLIGADOS" A ORGANISMOS CIUDADANOS, INSTITUCIONES PRIVADAS Y ORGANISMOS NO GUBERNAMENTALES QUE RECIBAN, ADMINISTREN O APLIQUEN RECURSOS PÚBLICOS, CONTRAVIENE EL ARTÍCULO 6o. DE LA CONSTITUCIÓN FEDERAL. Tesis: III.2o.T.Aux.2 A, Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XXXI, marzo de 2010, p. 3086.

derecho deberá prevalecer el principio de máxima publicidad.	fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público y seguridad nacional, en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad. Los sujetos obligados deberán documentar todo acto que derive del ejercicio de sus facultades, competencias o funciones, la ley determinará los supuestos específicos bajo los cuales procederá la declaración de inexistencia de la información.

Entonces, como se puede apreciar, la interpretación en 2010 era correcta al advertirse que los sujetos obligados estaban limitados a entes de carácter público; y con la reforma de 2014, la base de sujetos obligados fue ampliada, tal como se aprecia a continuación:

ENTIDAD FEDERATIVA	TEXTO EN LA CONSTITUCIÓN LOCAL
AGUASCALIENTES	No se indica expresamente quienes son sujetos obligados, sin embargo, en su artículo 62-A, solo menciona el derecho de acceso a la información y el fundamento de su autoridad garante.
BAJA CALIFORNIA	Artículo 7.- […] APARTADO C. De la Transparencia y Acceso a la Información Pública. […] Para el ejercicio del derecho de acceso a la información, deberán atenderse las siguientes bases: I.- Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito estatal y municipal, es pública y sólo podrá ser reservada temporalmente por las razones de interés público en los términos que fije la

ENTIDAD FEDERATIVA	TEXTO EN LA CONSTITUCIÓN LOCAL
BAJA CALIFORNIA SUR	Ley. 7°. […] B.- […] Para proteger el derecho fundamental de acceso a la información, se establecen los siguientes criterios, principios y bases: I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, Municipios, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público y seguridad publica en los términos que fijen las leyes. En la interpretación y aplicación de este derecho deberá prevalecer el principio de máxima publicidad.
CAMPECHE	ARTÍCULO 125 bis.- En el Estado de Campeche se contará con un organismo autónomo, especializado, imparcial y colegiado, responsable de garantizar el derecho de acceso a la información y de protección de 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, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en los ámbitos estatal y municipal.
COAHUILA	No se indica expresamente quienes son sujetos obligados, sin embargo, en sus artículos 7° y 8°, solo menciona el derecho de acceso a la información y el fundamento de su autoridad garante.
COLIMA	Artículo 5° [..] B. [..] En la interpretación del derecho de acceso a la información deberá prevalecer el principio de máxima publicidad y su ejercicio se regirá por los siguientes principios y bases: I. Toda la información en posesión de cualquier autoridad, entidad, órgano u organismo de los poderes Ejecutivo, Legislativo y Judicial del Estado, de los municipios, órganos autónomos, partidos políticos, fideicomisos y fondos

ENTIDAD FEDERATIVA	TEXTO EN LA CONSTITUCIÓN LOCAL
	públicos, así como de cualquier persona física, moral o sindicato, que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito del Estado y los municipios, es pública y sólo podrá ser reservada temporalmente por razones de interés público y seguridad, en los términos que fijen las leyes;
CHIAPAS	No se indica expresamente quienes son sujetos obligados, sin embargo, en sus artículos 5° XV, 62, y 102, solo mencionan el derecho de acceso a la información y el fundamento de su autoridad garante.
CHIHUAHUA	Artículo 4º. III. Para el ejercicio del derecho de acceso a la información, se estará a los principios y bases a que se refiere el artículo 6º. de la Constitución Política del los Estados Unidos Mexicanos.
CDMX	Artículo 7.- Ciudad Democrática […] D. Derecho a la información[…] 2. Se garantiza el acceso a la información pública que posea, transforme o genere cualquier instancia pública, o privada que reciba o ejerza recursos públicos o realice actos de autoridad o de interés público. Esta información deberá estar disponible en formatos de datos abiertos, de diseño universal y accesibles.
DURANGO	ARTÍCULO 29.- El derecho a la información está garantizado en los términos de la presente Constitución y de la Constitución Política de los Estados Unidos Mexicanos. Se regirá por los siguientes principios: I. Toda la información gubernamental es pública, los poderes del Estado, ayuntamientos, cualquier otro organismo, dependencia o entidad estatal o municipal, órganos constitucionales autónomos, concesionarios de bienes y servicios, partidos políticos, sindicatos, universidades, fideicomisos y fondos públicos, y cualquier persona física o moral que reciba recursos públicos o que realicen actos de autoridad están obligados a proporcionarla, sólo podrá ser reservada de manera temporal, en los términos que fije la ley, debiendo prevalecer el principio de máxima publicidad. II. Las personas físicas o jurídicas de derecho privado que reciban, usen, administren y ejerzan recursos públicos, están obligadas a proporcionar la información relativa a éstos.

ENTIDAD FEDERATIVA	TEXTO EN LA CONSTITUCIÓN LOCAL
GUANAJUATO	Artículo 14. […] B […] Para el ejercicio del derecho de acceso a la información, los Poderes, organismos autónomos y ayuntamientos, en el ámbito de sus respectivas competencias, se regirán por las siguientes fracciones y bases: I. Toda la información pública en posesión de los poderes ejecutivo, legislativo o judicial y de cualquier autoridad, órgano estatal y municipal, incluyendo los órganos autónomos por disposición constitucional, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público, seguridad nacional y seguridad pública en los términos que fijen las leyes
GUERRERO	Artículo 120. […] Son sujetos obligados por la Ley de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Guerrero y, en consecuencia, competencia del Instituto, cualquier autoridad, entidad, órgano u organismos de los Poderes Legislativo, Ejecutivo y Judicial, Órganos Autónomos, Órganos con Autonomía Técnica, los Ayuntamientos, partidos políticos, candidatos independientes, fideicomisos y fondos públicos, instituciones de educación básica, media, media superior, superior y de posgrado; centros de investigación, así como cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en los ámbitos estatal y municipal.
HIDALGO	Artículo 4 Bis. […] El derecho de acceso a la información pública, se regirá por los siguientes principios: I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial del Estado, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito estatal y

ENTIDAD FEDERATIVA	TEXTO EN LA CONSTITUCIÓN LOCAL
	municipal, a quienes se les denominará sujetos obligados, es pública y sólo podrá ser reservada temporalmente por las razones y en los términos que señalen las leyes. Artículo 15.- […] X. […] La ley regulará el ejercicio del derecho a la información pública y el procedimiento para hacerlo efectivo; las obligaciones por parte de los sujetos de aplicación de la ley respecto a la transparencia y el derecho a la información pública, así como las sanciones por su incumplimiento, de conformidad con lo establecido por la Constitución Política de los Estados Unidos Mexicanos, la Ley General de Transparencia y Acceso a la Información Pública, esta Constitución y demás normatividad aplicable en la materia.
JALISCO	Será obligación de las autoridades estatales y municipales, de cualquier otro organismo público, así como de cualquier persona física, jurídica o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad, proporcionar la información pública en su posesión, rendir cuantas de sus funciones y permitir el ejercicio del derecho a la información en los términos de la ley. Artículo 5.- […] I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismos de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos estatales y municipales, así como del gobierno y de la administración pública municipal y sus organismos descentralizados, asimismo de cualquier persona física, jurídica colectiva o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones previstas en la Constitución Política de los Estados Unidos Mexicanos de interés público y seguridad, en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad. Los sujetos obligados deberán documentar todo acto que derive del ejercicio de sus facultades,
MEXICO	

ENTIDAD FEDERATIVA	TEXTO EN LA CONSTITUCIÓN LOCAL
MICHOACAN	competencias o funciones, la ley determinará los supuestos específicos bajo los cuales procederá la declaración de inexistencia de la información. Artículo 8°. […] Toda persona tendrá derecho al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión, el que se regirá por los siguientes principios y bases: I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público y seguridad nacional, en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad. Los sujetos obligados deberán documentar todo acto que derive del ejercicio de sus facultades, competencias o funciones, la ley determinará los supuestos específicos bajo los cuales procederá la declaración de inexistencia de la información;
MORELOS	ARTÍCULO 2.- […] Para el ejercicio del derecho de acceso a la información, el Estado y los municipios, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases: I. Toda la información en posesión de los poderes públicos estatales, autoridades municipales, organismos públicos autónomos creados por esta Constitución, organismos auxiliares de la administración pública estatal o municipal, partidos políticos, fondos públicos, personas físicas, morales o sindicatos que reciben y ejerzan recursos públicos o realicen actos de autoridad en el ámbito estatal y municipal y, en general, de cualquier órgano de la Administración Pública del Estado es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes. […]

ENTIDAD FEDERATIVA	TEXTO EN LA CONSTITUCIÓN LOCAL
NAYARIT	ARTÍCULO 7.- […] XII. El derecho de acceso a la información pública y a la transparencia. La información en posesión de los sujetos obligados se regirá conforme a los principios de máxima publicidad y expedites, sin más limitaciones que las relativas a los datos personales o la información que sea declarada reservada o confidencial, en los términos que disponga la ley.
NUEVO LEON	Art. 6o.- […] El ejercicio del derecho de acceso a la información, se regirá bajo los siguientes principios y bases: I.- Toda la información en posesión de cualquier autoridad, dependencia, unidades administrativas, entidad, órgano u organismo municipal o de los Poderes Ejecutivo, Legislativo, Judicial o del ámbito municipal, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito estatal y municipal, es pública, y sólo podrá ser reservada temporalmente por razones de interés público y seguridad nacional, en los términos que fijen las Leyes. […]
OAXACA	Artículo 3.-[…] Para el ejercicio del derecho de acceso a la información, el Estado y los Municipios, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases: I.- Es pública toda la información en posesión de cualquier autoridad, entidad y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos del Estado, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito estatal y municipal.
PUEBLA	Artículo 12. Las leyes se ocuparán de: VII. Garantizar el acceso a la información pública en posesión de cualquier autoridad, entidad, órgano y organismo de

ENTIDAD FEDERATIVA	TEXTO EN LA CONSTITUCIÓN LOCAL
	los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito estatal y municipal, así como de proteger los datos personales y la información relativa a la vida privada, en los términos y con las excepciones que establezca la Constitución Política de los Estados Unidos Mexicanos, la Ley General de Transparencia y Acceso a la Información Pública y la Ley aplicable a la materia. El ejercicio del derecho de acceso a la información se regirá por los siguientes principios: a) Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público, en los términos que fijen las leyes.
QUERETARO	No se indica expresamente quienes son sujetos obligados, sin embargo, en sus artículos 33 Apartado B, 62, y 102, solo mencionan el derecho de acceso a la información y el fundamento de su autoridad garante.
QUINTANA ROO	Artículo 21.- […] Para el ejercicio del derecho de acceso a la información, regirán los principios y bases siguientes: I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, Municipios, órganos públicos autónomos, partidos políticos, fideicomisos y fondos públicos, así como cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés

ENTIDAD FEDERATIVA	TEXTO EN LA CONSTITUCIÓN LOCAL
	público y seguridad nacional, estatal o municipal, en términos que fijen las leyes.
SAN LUIS POTOSI	No se indica expresamente quienes son sujetos obligados, sin embargo, en su artículo 17 fracción III, se mencionan el derecho de acceso a la información y el fundamento de su autoridad garante.
SINALOA	Art. 109 Bis B. Se garantiza en el Estado el derecho de acceso a la información pública a toda persona, en los términos de la ley respectiva. […] El ejercicio de este derecho se regirá por los principios y bases consagrados en al artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos.
SONORA	ARTICULO 2o.- […] En materia de información pública: APARTADO A.- El Estado de Sonora reconoce el derecho humano de toda persona al libre acceso a la información veraz, verificable, confiable, actualizada, accesible, comprensible y oportuna. Comprende su facultad para solicitar, buscar, difundir, investigar y recibir información. Es obligación de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, incluidas sociedades, organizaciones e instituciones de derecho privado con participación estatal y municipal, así como cualquier persona física, moral o sindicato que reciba, administre y ejerza recursos públicos o realice actos de autoridad en el ámbito estatal y municipal, para garantizar el libre ejercicio de este derecho, para difundir y hacer del conocimiento público la información que se le solicite así como poner a disposición las obligaciones de transparencia y toda aquella información que se considere de interés público que fijen las leyes.
TABASCO	Artículo 4 bis.- El derecho a la información es inherente al ser humano y por lo tanto el Estado tiene la obligación primigenia de reconocerlo y garantizarlo, tomando en consideración los siguientes principios: I. Es información pública la generada o en posesión de cualquier autoridad, entidad, órgano y organismo estatal o municipal, así como de las personas físicas o

ENTIDAD FEDERATIVA	TEXTO EN LA CONSTITUCIÓN LOCAL
TAMAULIPAS	jurídicas colectivas que reciban recursos públicos, cuando esté directamente relacionada con el ejercicio de éstos; ARTÍCULO 17.- El Estado reconoce a sus habitantes: […] V.- La libertad de información y, en particular de sus ciudadanos para asuntos políticos, así como para utilizar y divulgar la información pública que reciban. El Estado garantizará el acceso a la información pública. Todo ente público, entidad, órgano y organismo de los Poderes Legislativo, Ejecutivo y Judicial, y municipios; órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito estatal y municipal; respetará esta libertad y pondrá a disposición del público la información con que cuente en virtud de sus actividades; salvo aquellas excepciones que se señalen expresamente en las leyes de la materia, o aquellas relativas a la intimidad, privacidad y dignidad de las personas, en los términos que señale la ley. La libertad de información comprende la protección del secreto profesional, sin demérito del derecho de réplica de toda persona ante la divulgación de información inexacta que le agravie.
TLAXCALA	ARTICULO 19.- Son derechos Humanos, los que en forma enunciativa y no limitativa se enlistan: V. El Estado garantizará el derecho a la información. Toda persona ejercerá su derecho de acceso a la información que se encuentre en poder de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito estatal y municipal, mediante los principios y bases siguientes: a) Toda la información en posesión de los sujetos obligados, es pública y sólo podrá ser reservada temporalmente por razones de interés público y seguridad nacional en los términos que fije la ley de la materia. […]

ENTIDAD FEDERATIVA	TEXTO EN LA CONSTITUCIÓN LOCAL
VERACRUZ DE IGNACIO DE LA LLAVE	Artículo 6. […] En el Estado, los poderes públicos, organismos autónomos, ayuntamientos o concejos municipales, entidades paraestatales y paramunicipales creadas por uno o más ayuntamientos, organizaciones políticas; los fideicomisos, fondos públicos y sindicatos de cualquiera de éstos, además de toda persona física o moral que reciba y ejerza recursos públicos, así como aquellas que realicen actos de autoridad o que desempeñen funciones o servicios públicos, son sujetos obligados en materia de acceso a la información y de protección de datos personales que obren en su posesión, en los términos de esta Constitución y la ley.
YUCATAN	Artículo 75.- […] El Instituto Estatal de Transparencia, Acceso a la Información Pública y Protección de Datos Personales tiene competencia para conocer de los asuntos relacionados con el acceso a la información pública y la protección de datos personales en posesión o a cargo de cualquier autoridad, entidad, órgano u organismo de los poderes Ejecutivo, Legislativo y Judicial, ayuntamientos, órganos autónomos, partidos políticos estatales y nacionales con registro en el estado, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito estatal o municipal.
ZACATECAS	Artículo 29. […] Para el ejercicio del derecho de acceso a la información, el Estado y los Municipios, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases: I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo, Judicial y de los Municipios, organismos autónomos, partidos políticos, fideicomisos, fondos públicos y asociaciones civiles, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito,

ENTIDAD FEDERATIVA	TEXTO EN LA CONSTITUCIÓN LOCAL
	estatal o municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público, en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad. Los sujetos obligados deberán documentar todo acto que derive del ejercicio de sus facultades, competencias o funciones, la ley determinará los supuestos específicos bajo los cuales procederá la declaración de inexistencia de la información

Además, los sujetos obligados tienen el deber de proteger la confidencialidad de los datos personales bajo su poder, de recabar el consentimiento del titular previo al tratamiento, y de garantizar que toda persona pueda ejercer el derecho a la protección de sus datos personales, de lo contrario, deberán abstenerse de divulgar esa información.[246]

3.3 Responsables en Materia de Transparencia y Acceso a la Información

3.3.1 Sistema Nacional de Transparencia

El Sistema Nacional de Transparencia (SNT) tuvo como antecedente a la Conferencia Mexicana para el Acceso a la Información Pública, la cual se conformó por todos los titulares de los organismos vigilantes del acceso a la información en las entidades federativas.

Dentro de sus principios estuvieron:

- Establecer un esquema de cooperación y coordinación con los sujetos obligados en los ámbitos federal, estatal y municipal, en apego a los principios de transparencia y publicidad de su información.
- Propiciar y fomentar la cultura de transparencia, acceso a la información pública y rendición de cuentas.
- Promover e impulsar la promulgación de leyes y reformas que garanticen el derecho de acceso a la información pública que generen, posean o administren los sujetos obligados, así como la protección de datos personales.

[246] TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA EN EL ESTADO DE JALISCO. LA LEY RELATIVA Y EL REGLAMENTO DEL MUNICIPIO DE GUADALAJARA NO TRANSGREDEN EL DERECHO DE AUDIENCIA PREVIA PREVISTO EN EL ARTÍCULO 14 CONSTITUCIONAL. Tesis: PC.III.A. J/6 A (11a.) Semanario Judicial de la Federación, Undécima Época, t. II, diciembre de 2021, p. 2124.

- Fomentar y difundir la cultura del derecho a la confidencialidad y protección que requiere el tratamiento de los datos personales y, en su caco, actualizarlos en forma expedita.
- Impulsar y difundir entre los sujetos obligados criterios para la sistematización y conservación de archivos que permitan localizar eficientemente la información pública.
- Promover y establecer relaciones de colaboración y apoyo con organizaciones sociales, privadas e instituciones académicas nacionales o extranjeras, que contribuyan al fortalecimiento de la cultura de la transparencia, la rendición de cuentas y el derecho de acceso a la información.
- Impulsar el uso de nuevas tecnologías para facilitar el acceso a la información.[247]

La COMAIP estuvo funcionando desde el 16 de junio de 2004 hasta el 20 de junio de 2015.[248]

En la actual Ley General de Transparencia y Acceso a la Información Pública (LGTAI), se puede advertir, que dentro de sus objetivos está el de regular la organización y funcionamiento del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, así como establecer las bases de coordinación entre sus integrantes.[249]

El SNT está regulado en las siguientes disposiciones:

1. LGTAI, Título Segundo, Capítulo I, Del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales; artículos 27 a 36.
2. Ley Federal de Transparencia y Acceso a la Información Pública; artículo 39, 106, 107.
3. Reglamento del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.
    a. Acuerdo mediante el cual se reforma el artículo17 del Reglamento del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.
4. Lineamientos para la Organización, Coordinación y Funcionamiento de las Instancias de los Integrantes del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.
5. Lineamientos para la elección y/o Reelección de Coordinaciones de Comisiones, de las Regiones y Coordinación de los Organismos Garantes.

[247] Sistema Nacional de Transparencia, *Acta Constitutiva de la Conferencia Mexicana para el Acceso a la Información Pública (COMAIP)*, [en línea] México, SNT-INAI, 2004, [fecha de consulta: 3 de diciembre de 2022], Disponible en: *https://snt.org.mx/wp-content/uploads/2021/09/acta_comaip.pdf*
[248] Sistema Nacional de Transparencia, *Antecedentes*, México, SNT, s/a, [fecha de consulta: 3 de diciembre de 2022], Disponible en *https://snt.org.mx/?page_id=475*
[249] Artículo 2, fracción VI, LGTAI.

La finalidad del Sistema Nacional, de conformidad con el artículo 28 de la Ley, es la de coordinar y evaluar las acciones relativas a la política pública transversal de transparencia, acceso a la información y protección de datos personales, así como establecer e implementar los criterios y lineamientos que determine la Ley y demás normatividad aplicable.

A su vez, de acuerdo con el artículo 30 de la actual Ley Federal de Transparencia y Acceso a la Información Pública (LFTAI), son parte integrante del Sistema Nacional:

I. El Instituto [INAI];
II. Los Organismos garantes de las Entidades Federativas;
III. La Auditoría Superior de la Federación;
IV. El Archivo General de la Nación, y
V. El Instituto Nacional de Estadística y Geografía.

A su vez, el Sistema cuenta con una serie de instancias, mismas que están reglamentadas en los Lineamientos para la Organización, Coordinación y Funcionamiento de las Instancias de los Integrantes del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

En dichos lineamientos se establece que los integrantes del Sistema Nacional pueden participar en los siguientes espacios de coordinación, colaboración, diálogo, discusión, deliberación, análisis y propuestas:
I. Sesión de Trabajo de los integrantes del Sistema Nacional;
II. Sesión Regional;
III. Sesión de Comisiones, y
IV. Grupos de Trabajo.
Asimismo, los cuatro espacios deliberativos a arriba mencionados, serán coordinados, según corresponda por:
I. La Presidencia del Consejo Nacional;
II. La Secretaría Ejecutiva del Sistema Nacional;
III. Coordinación de los Organismos Garantes de las Entidades Federativas;
IV. Coordinación Regional;
V. Secretaría Regional;
VI. Coordinación de Comisión, y
VII. Secretarías de Comisiones.

Los Organismos Garantes están actualmente organizados por regiones, las cuales tienen un coordinador y un secretario.[250]

[250] Sistema Nacional de Transparencia, *Regiones*, [en línea], México, SNT-INAI, s.a., [fecha de consulta: 3 de diciembre de 2022], Disponible en: *https://snt.org.mx/?page_id=465*

Región	Entidades Federativas
	Ciudad de México, Guerrero, Hidalgo, Estado de México, Morelos, Oaxaca, Puebla y Tlaxcala.
	Baja California, Baja California Sur, Chihuahua, Coahuila, Durango, Nuevo León, Sinaloa, Sonora y Tamaulipas.
	Aguascalientes, Colima, Guanajuato, Jalisco, Michoacán, Nayarit, Querétaro, San Luis Potosí y Zacatecas.
	Veracruz, Tabasco, Campeche, Chiapas, Yucatán y Quintana Roo.

Por otra parte, las Comisiones del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, son instancias de trabajo de carácter especial u ordinario, especializadas, conformadas por integrantes del Sistema Nacional para coordinar, colaborar, dialogar, discutir, deliberar, analizar y dictaminar asuntos y temas de interés en las materias del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Las Comisiones podrán analizar, debatir y dictaminar asuntos en el seno de sus propias sesiones o en el marco de una reunión multidisciplinaria con alguna otra u otras Comisiones en el marco de una Sesión de Comisiones Unidas.

Para el adecuado desarrollo de las actividades del Sistema Nacional, se constituirán las siguientes comisiones ordinarias:

I. Comisión Jurídica, de Criterios y Resoluciones;
II. Comisión de Protección de Datos Personales;
III. Comisión de Capacitación, Educación y Cultura;
IV. Comisión de Vinculación, Promoción, Difusión y Comunicación Social;
V. Comisión de Tecnologías de la Información y Plataforma Nacional de Transparencia;
VI. Comisión de Archivos y Gestión Documental;
VII. Comisión de Gobierno Abierto y de Transparencia Proactiva;
VIII. Comisión de Asuntos de Entidades Federativas y Municipios;
IX. Comisión de Indicadores, Evaluación e Investigación;
X. Comisión de Derechos Humanos, Equidad de Género e Inclusión Social, y
XI. Comisión de Rendición de Cuentas

3.3.2. Consejo Nacional

Con la entrada en vigor de la nueva LGTAI, el artículo undécimo transitorio dispuso que el Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales debía instalarse a más tardar en sesenta días naturales, a partir de la entrada en vigor del Decreto; por lo que derivado de esta disposición, el 23 de junio de 2015 se llevó a cabo la Sesión de instalación del Consejo del Sistema, en la cual se aprobaron las Bases de Coordinación y Colaboración para la Implementación del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales; así como la Declaratoria del Consejo Nacional del mismo Sistema.[251]

Con base en el Reglamento del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la información Pública y Protección de Datos Personales, el Consejo Nacional es el órgano colegiado y máximo rector de coordinación y deliberación del Sistema Nacional. Regirá su funcionamiento bajo los principios de certeza, eficacia, independencia, legalidad, objetividad, profesionalismo, máxima publicidad y transparencia.

En dicho reglamento, se dispone que el Consejo Nacional tiene las facultades y atribuciones siguientes:

I. Emitir acuerdos y resoluciones generales para el funcionamiento del Sistema Nacional con efectos vinculantes para todos sus integrantes;
II. Establecer reglamentos, lineamientos, criterios y demás instrumentos normativos necesarios para cumplir con los objetivos del Sistema Nacional, la Plataforma Nacional y la Ley;
III. Establecer indicadores, metas, estrategias, códigos de buenas prácticas, pronunciamientos, declaraciones, modelos y políticas tendientes a cumplir

[251] Sistema Nacional de Transparencia, *Acta de la Reunión de Instalación*, *ACT/23/06/2015*, [en línea] México, SNT, 23 de junio de 2015, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://snt.org.mx/wp-content/uploads/2021/08/ACTA-de-la-Reunion-de-Instalacion-23junio2015.pdf*

con los objetivos del Sistema Nacional y la Ley;
IV. Aprobar, ejecutar y evaluar el Programa Nacional e informar al Sistema Nacional sobre el resultado de estas acciones;
V. Establecer programas de alcance nacional para la promoción, investigación, diagnóstico y difusión en materias de transparencia, acceso a la información, protección de datos personales y apertura gubernamental en el país;
VI. Establecer los criterios para la publicación de los indicadores que permitan a los sujetos obligados rendir cuentas del cumplimiento de sus objetivos y resultados obtenidos;
VII. Emitir acuerdos para dar cumplimiento a las funciones del Sistema Nacional establecidas en el artículo 31 de la Ley;
VIII. Coordinar de forma efectiva las instancias que integran el Sistema Nacional;
IX. Establecer Comisiones con un propósito específico a fin de atender los temas o asuntos que les encomiende el Consejo Nacional;
X. Reformar, adicionar, derogar o abrogar los acuerdos aprobados y resolver todos los asuntos no previstos por éstos.

Asimismo, dentro de las acciones más importantes del Consejo es la de definir las reglas básicas del Programa Nacional de Transparencia y Acceso a la Información (PROTAI)

El PROTAI, tiene por objetivo general fortalecer el cumplimiento normativo, la difusión, la capacitación, la profesionalización y los procedimientos institucionales de la garantía progresiva del derecho de acceso a la información, la transparencia y la rendición de cuentas, al dar trascendencia nacional de los mismos a través del trabajo organizado y la influencia que ejercen el INAI, las instituciones federales integrantes del SNT y los organismos garantes de las entidades federativas, en su ámbito de competencia sobre los sujetos obligados de las leyes en la materia.

Cabe señalar que el PROTAI no es una nueva regulación, norma o lineamiento. En contraste, el PROTAI organiza por prioridades y simplifica el trabajo generado por las obligaciones, funciones y facultades existentes en las normas. El PROTAI tuvo una vigencia de 2017 a 2021.

De acuerdo con el PROTAI, la cantidad de normas vinculadas a los temas de acceso a la información son los siguientes:

- 6 leyes generales
- 5 leyes federales y al menos 124 leyes estatales
- 2 reglamentos (del Consejo Nacional del SNT y de la LFA)
- 11 lineamientos
- 6 acuerdos
- 5 guías
- 3 instructivos (sobre archivos en la APF)

- 2 recomendaciones (sobre archivos en la APF)
- 2 normas (sobre archivos en la APF)
- 1 decreto (sobre datos abiertos en la APF)

Asimismo, en cuanto a la cantidad de funciones, obligaciones y sujetos tenemos lo siguiente: 9 objetivos (LGTAIP)

- 13 obligaciones de sujetos obligados (LGTAIP)
- 14 funciones del SNT (LGTAIP)
- 4 integrantes federales del SNT
- 32 integrantes locales del SNT
- 21 atribuciones de los organismos garantes (LGTAIP)
- 8 funciones de los organismos garantes en materia de promoción de la transparencia y del DAI
- 8 funciones de los Comités de Transparencia (LGTAIP)
- 11 funciones de las Unidades de Transparencia (LGTAIP)
- 48 obligaciones de transparencia comunes (LGTAIP)
- 42 fracciones adicionales dentro de las obligaciones de transparencia comunes
- 122 obligaciones de transparencia específicas (LGTAIP)
- 51 fracciones adicionales dentro de las obligaciones de transparencia específicas
- 3,249 criterios de publicación y actualización de obligaciones de transparencia (DOF 04-05-2016)
- 32 leyes locales de transparencia
    - 17 atribuciones para los sujetos obligados en promedio
    - 35 atribuciones para los organismos garantes en promedio
    - 50 obligaciones de transparencia comunes en promedio
    - 14 obligaciones de las Unidades de Transparencia en promedio
    - 11 obligaciones de los Comités de Transparencia en promedio
- 882 sujetos obligados en el ámbito federal
- 7,259 sujetos obligados en el ámbito local

3.3.3. Organismos Garantes

La protección de los derechos de acceso a la información, datos personales y rendición de cuentas, no se protegen ni garantizan solamente por la buena fe de aquellos denominados sujetos obligados. La historia nos demuestra que la denominada “autoridad”, tienen por excelencia la “necesidad” de “ocultar” determinada información por “razones de Estado”.

En México, vimos que a pesar de la denominada Reforma Política de los 70´s, donde se plasmó que la información sería garantizada por el Estado; no tuvo la fuerza necesaria, lo que ocasionaría ver comprometida, no solamente la credibilidad del Estado mexicano, sino también una estabilidad política e institucional.

La ciudadanía a lo largo de las décadas, pidió y pidió rendición de cuentas claras, que dejara de existir la "opacidad" con la que la autoridad se conducía y solo hasta la alternancia presidencial del año 2000 además de presiones internacionales y casos escandalosos como los de aguas blancas, hicieron que por fin se diseñara una nueva estructura que diera paso a que la ciudadanía estuviera mejor enterada de las acciones de gobierno; pero, faltaba la institución que sería la encargada de salvaguardar las garantías consagradas en materia de transparencia..

Para ello se creó el entonces IFAI (ahora INAI), como organismo garante para la federación con alcance nacional y 32 organismos estatales, correspondientes a cada una de las entidades federativas. Esto también modificó la estructura de las funciones clásicas estatales. A decir del Dr. Fernández Ruiz:

> "resulta ser de muy difícil acotamiento y precisión, lo cual ha llevado a algunos autores a tratar de definir por exclusión de la función legislativa y de la jurisdiccional, al decir que será administrativa toda función pública diferente de la legislativa y judicial, lo que dista mucho de determinar su género próximo y diferencia específica, aunado a lo cual, la aparición de funciones administrativas emergentes, como la contralora, la electoral, la de regulación monetaria y la registral, hacen actualmente inaceptable ese procedimiento definitorio."[252]

Autores como Manuel García Pelayo, comenta que con un enfoque "maximalista" que los órganos constitucionales autónomos serán aquello que cumplan con cuatro características: [253]

1) Rango Constitucional.
    a. Se debe especificar su composición.
    b. Métodos de designación de sus titulares.
    c. Sistemas de competencias.
    d. Estatus Jurídico.
2) Participación en la dirección política del Estado.
    a. Necesarios para el buen funcionamiento del "modelo de Estado".
    b. Si desaparece, se trastoca la "sustancialidad" o la "globalidad" del sistema. constitucional vigente.
3) Presencia constitutiva y.
    a. Toman decisiones por y en nombre del Estado que vinculen o que comprometan a la sociedad nacional.
4) Relaciones de coordinación con otros poderes.

---

[252] Fernández Ruiz, Jorge, *Apuntes para una Teoría Jurídica de las Actividades del Estado*, [en línea], México, IIJ-UNAM, Boletín Mexicano de Derecho Comparado No. 99, septiembre – diciembre 2000, [fecha de consulta: 3 de diciembre de 2022] Disponible en:
http://historico.juridicas.unam.mx/publica/rev/boletin/cont/99/art/art1.htm

[253] Ackerman, John M., *Organismos Autónomos y la nueva división de poderes en México y América Latina*, en "Homenaje al Doctor Emilio O. Rabasa", [en línea], México, IIJ-UNAM, 2016, [fecha de consulta: 3 de diciembre de 2022] Disponible en:
https://archivos.juridicas.unam.mx/www/bjv/libros/6/2834/5.pdf p. 5.

a. Tienen paridad de rango; es decir, no están subordinados a ningún otro poder.
b. Mantiene una coordinación constante y regulada por la Constitución con otros órganos constitucionales.

Así como existe el criterio "maximalista" existe otro criterio, llamado "minimalista", el cual consiste en que un organismo expresamente mencionado en la Constitución "que no forma parte de uno de los tres poderes tradicionales del Estado sería automáticamente un organismo constitucional autónomo".[254]

Ileana Moreno define a los organismos autónomos como "entes jurídicos de derecho público de carácter atípico, que no dependen orgánicamente de ninguna de las tres ramas tradicionales".[255]

Por su parte, el Tribunal en pleno de la Suprema Corte de Justicia de la Nación ha sostenido lo siguiente:

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

[254] *Ídem*.
[255] *Ibidem*, p. 10.

ser eficazmente atendidas en beneficio de la sociedad.[256]

Con motivo de la evolución del concepto de distribución del poder público se han introducido en el sistema jurídico mexicano, a través de diversas reformas constitucionales, órganos autónomos cuya actuación no está sujeta ni atribuida a los depositarios tradicionales del poder público (Poderes Legislativo, Ejecutivo y Judicial), a los que se les han encargado funciones estatales específicas, con el fin de obtener una mayor especialización, agilización, control y transparencia para atender eficazmente las demandas sociales; sin que con ello se altere o destruya la tradicional doctrina de la división de poderes, pues la circunstancia de que los referidos organismos guarden autonomía e independencia de los poderes primarios, no significa que no formen parte del Estado mexicano, ya que 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.

Ahora bien, aun cuando no existe algún precepto constitucional que regule la existencia de los órganos constitucionales autónomos, éstos deben:

a) Estar establecidos y configurados directamente en la Constitución;
b) Mantener con los otros órganos del Estado relaciones de coordinación;
c) Contar con autonomía e independencia funcional y financiera; y,
d) Atender funciones coyunturales del Estado que requieran ser eficazmente atendidas en beneficio de la sociedad.[257]

Con base en estas interpretaciones de la SCJN, y con la concepción del Dr. Jorge Fernández Ruiz, se puede contemplar una nueva forma de entender la actuación de la función administrativa. Por lo tanto, en este nuevo esquema los Organismos Constitucionales Autónomos u OCA´s, generan una nueva forma de entender las relaciones de poder en el Estado.

En este sentido, el marco constitucional y legal que rige al ahora INAI, “lo coloca como intermediario entre las autoridades y la sociedad para que la información pública se constituya en el insumo que genere procesos de rendición de cuentas y lógicas de colaboración entre ellos. Además, le otorga atribuciones de autonomía y sanción que lo fortalecen y le obligan a impulsar el Gobierno abierto en el país”.[258]

La tarea de los órganos garantes es la de buscar una mayor apertura en el

[256] ÓRGANOS CONSTITUCIONALES AUTÓNOMOS. NOTAS DISTINTIVAS Y CARACTERÍSTICAS. Tesis: P./J. 20/2007, Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XXV, mayo de 2007, p. 1647.

[257] ÓRGANOS CONSTITUCIONALES AUTÓNOMOS. SUS CARACTERÍSTICAS. Tesis: P./J. 12/2008, Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XXVII, febrero de 2008, p. 1871.

[258] Salas Juárez, Joel, *El papel de los órganos garantes del acceso a la información pública en el contexto del Estado Abierto*, en “Desde el gobierno abierto al Estado abierto en América Latina y el Caribe”, [en línea] Chile, CEPAL, 2017, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://archivos.juridicas.unam.mx/www/bjv/libros/10/4686/28.pdf* p. 152.

denominado Gobierno Abierto (Tema que se abordará con posterioridad); el cual a su vez refiere a otro tema de igual importancia que es el de la gobernanza, mismo que por su complejidad y aplicado al tema de transparencia y rendición de cuentas de manera horizontal, "se esperaría que los ciudadanos conocieran las circunstancias en que las autoridades toman las decisiones, así como las restricciones o facilidades para llevarlas a cabo, de modo que estarían en condiciones de evaluar la validez de dichas decisiones, exigir en consecuencia, proponer mejoras y colaborar en la solución de los problemas públicos."[259]

En este sentido los órganos garantes se convierten en intermediarios y una especie de "ombudsman" que media entre los ciudadanos y las autoridades o ahora sujetos obligados (incluyendo a particulares en determinados casos), cuando no se satisfagan las peticiones, o bien, cuando los sujetos obligados incumplan en sus obligaciones de transparencia y rendición de cuentas.

Hay que recordar que con la reforma constitucional de la primera década de este siglo la regulación en materia de transparencia era de manera coincidente; es decir, teníamos una Ley Federal y por otra parte, las entidades federativas regulaban lo conducente, lo que hizo que en un momento tuviéramos diferentes regulaciones. En el caso de los órganos garantes, el IFAI lo era en carácter federal, y las instituciones de transparencia locales lo eran en su ámbito de competencia territorial, aunque de *facto*, el IFAI era el órgano rector a nivel nacional.

Con la reforma del 2014 el IFAI se transformó en el INAI, lo anterior significó un cambio en el paradigma de entendimiento en materia de coordinación y colaboración entre los diversos órganos garantes. La transformación constitucional generó una nueva legislación con carácter concurrente; es decir, se creó una nueva Ley General, que implicó la creación de un sistema que permite una armonización en las legislaciones de carácter federal y local.

En este sentido el INAI se convirtió no solamente en un órgano constitucional autónomo sino en un ente regulador a nivel nacional con una amplia competencia en transparencia, rendición de cuentas coma datos personales y archivos; fortaleciendo el marco del federalismo mexicano.

De acuerdo con Joel Salas, el INAI ha trabajado en cuatro ámbitos:

1) Mantenimiento y avance de la dinámica o administración de la alianza para el Gobierno abierto en el país, dando continuidad pese a los cambios de autoridades.
2) Promoción del Gobierno abierto entre los 3 poderes (Ejecutivo, legislativo y judicial) y los 3 niveles de Gobierno (federal como estatal y municipal).
3) Definición e impulso de un modelo teórico que clarifique conceptos y criterios para establecer las características mínimas Del Gobierno abierto en el país.

[259] *Ibidem,* p. 58.

4) Puesta en práctica del modelo a nivel local.[260]

Por otra parte, los órganos garantes son los siguientes:

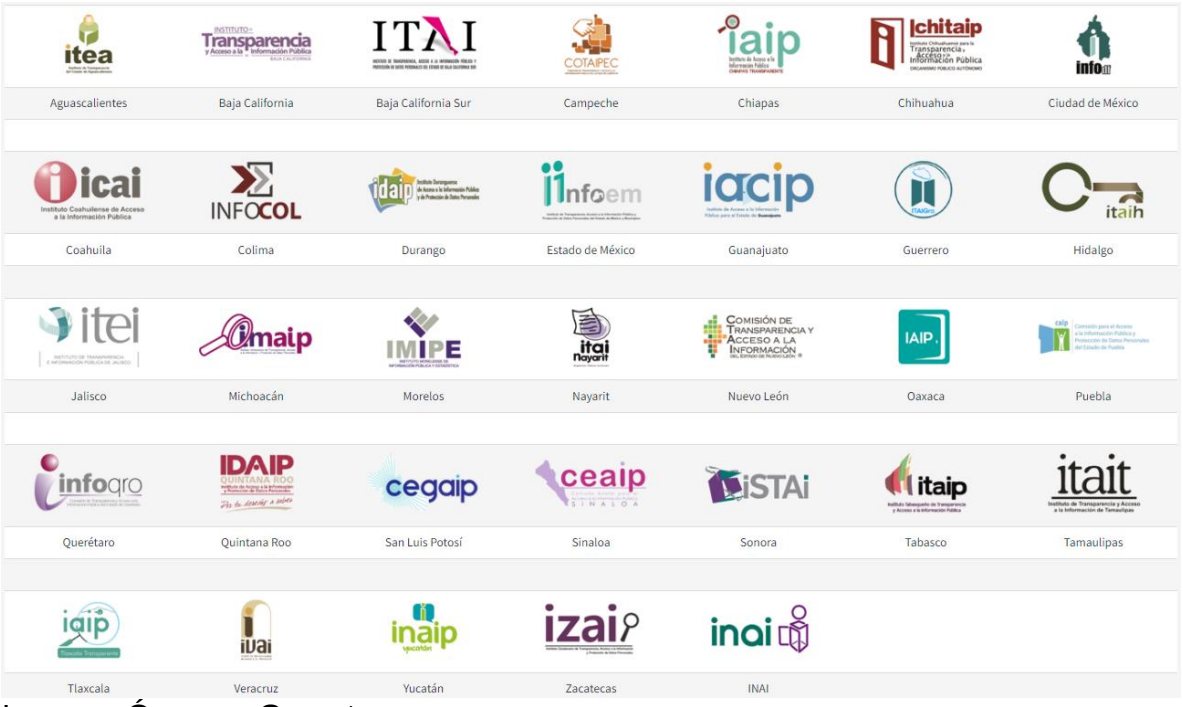


Imagen: Órganos Garantes.
Tomada de: INFOCDMX, *Órganos Garantes*, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://infocdmx.org.mx/index.php/transparencia-en-m%C3%A9xico/%C3%B3rganos-garantes.html*

Otra de las funciones más importantes es la de emitir los criterios de interpretación. Por ello el 03 de marzo de 2016, fueron publicados en el Diario Oficial de la Federación, los Lineamientos para la emisión de criterios de interpretación del INAI.

Los criterios de interpretación, tanto reiterados como relevantes, serán de carácter vinculante para los sujetos obligados en el ámbito federal y, orientadores para los organismos garantes de las entidades federativas.

En INAI, mediante diferentes acuerdos aprueban criterios de interpretación de acuerdo con los artículos 199 y 200 de la Ley General de Transparencia. Por ejemplo, en el Acuerdo ACT.-PUB/05/04/2017.06[261] de 05 de abril de 2017 se aprobaron los siguientes criterios:

[260] *Ibidem*. p. 161.
[261] INAI, *Acuerdo mediante el cual se aprueban los criterios de interpretación emitidos por Instituto Nacional de Transparencia, acceso a la Información y Protección de datos personales, en términos de los artículos 199 y 200 de la Ley General de Transparencia y Acceso a la Información Pública y 172 y 173 de la Ley Federal de Transparencia y Acceso a la Información Pública,* [en línea] México, INAI, 2017, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *http://criteriosdeinterpretacion.inai.org.mx/Documents/Acuerdo%20de%20aprobaci%C3%B3n%20de%20los%20criterios%20de%20interpretaci%C3%B3n.PDF*

- Criterio 01/17. Es Improcedente ampliar las solicitudes de acceso a información, a través de la interposición del recurso de revisión.
- Criterio 02/17. Congruencia y exhaustividad. Sus alcances para garantizar el derecho de acceso a la información.
- Criterio 03/17. No existe obligación de elaborar documentos *ad hoc* para atender las solicitudes de acceso a la información.
- Criterio 04/17. Resoluciones del Comité de Transparencia, gozan de validez siempre que contengan la firma de quine los emite.
- Criterio 05/17. La información patrimonial de personas morales de derecho público no lesional el bien jurídico tutelado que ampara el secreto fiscal.
- Criterio 06/17. Copias Certificadas, como modalidad de entrega en la Ley Federal de Transparencia y Acceso a la Información Pública corrobora que el documento es una copia fiel del que obra en los archivos del sujeto obligado.
- Criterio 07/17. Casos en los que no es necesario que el Comité de Transparencia confirme formalmente la inexistencia de la información.

Los criterios vigentes son los emitidos a partir del 2017, elaborados con base en la Ley General de Transparencia y Acceso a la Información Pública y la Ley Federal de Transparencia y Acceso a la Información Pública. Estos criterios son obligatorios para los sujetos obligados del ámbito federal y orientadores para los organismos garantes estatales.

Los criterios históricos fueron formulados entre los años 2009 al 2014, con fundamento en la abrogada Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Estos criterios sólo pueden utilizarse como referente para el tema que traten.
Un par de cuestiones adicionales:

Primero, que la actuación del INAI es reglada y no discrecional. Lo anterior, porque se está en presencia de una facultad reglada, al dar inicio a un procedimiento a instancia de parte, regulado en la ley de la materia, que debe culminar con el dictado de una resolución, y en el que, para la motivación de la sanción, deben tomarse en cuenta determinados presupuestos normativos. Esto es, el procedimiento que prepara o enmarca el dictado de una sanción no implica, *per se*, el ejercicio de facultades discrecionales, ya que es previo y preparatorio para ejercer el arbitrio sancionador. En consecuencia, el procedimiento en sus distintas fases, que culmina con una resolución en donde se valoran aspectos para individualizar la sanción, constituye un aspecto reglado, por lo que las violaciones durante él cometidas, son aquellas a que se refieren las fracciones II y III del artículo 51 de la Ley Federal de Procedimiento Contencioso Administrativo y la ilegalidad en que pueda incurrirse conlleva una nulidad para efectos, sin involucrar aún temas de fondo, los que se actualizan con el dictado de la sanción propiamente dicha.[262]

[262] FACULTADES DEL INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES (INAI). LAS EJERCIDAS AL IMPONER SANCIONES ECONÓMICAS, DERIVADO DE LA DENUNCIA PRESENTADA POR UN

Segundo. Que en materia de Datos Personales en Poder de Particulares es improcedente el Juicio Contencioso Administrativo Federal. La Segunda Sala de la Suprema Corte de Justicia de la Nación decidió vía jurisprudencia, que el juicio de nulidad es improcedente, porque de acuerdo con la reforma constitucional publicada en el Diario Oficial de la Federación el 7 de febrero de 2014, la única vía para combatir estas resoluciones es el juicio de amparo.

Es así, porque uno de los objetivos esenciales de la aludida reforma constitucional en materia de transparencia, fue que los particulares únicamente pudieran impugnar las resoluciones de dicho Instituto vía juicio de amparo, con la clara intención de no alargar los procedimientos en materia de acceso a la información y tutelar de mejor manera ese derecho; en ese sentido, si el Poder Reformador de la Constitución otorgó competencia al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales para conocer de la materia de protección de datos personales en posesión de los particulares, en tanto se determina la instancia responsable encargada de atender los temas en esa materia, debe entenderse derogado el artículo 56 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, porque al ser de contenido previo a la mencionada reforma, resulta contrario al marco constitucional y legal que lo rige en la actualidad, conforme al cual los particulares sólo pueden impugnar sus resoluciones a través del juicio de amparo.[263]

3.3.4. Comités de Transparencia

Los comités de transparencia son las máximas autoridades, tanto en materia de transparencia como en materia de protección de datos personales en posesión de sujetos obligados; dichos comités operan al interior por cada sujeto obligado.

El cuatro de mayo de dos mil quince, se publicó en el Diario Oficial de la Federación la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), la cual en su artículo 43 establece que cada sujeto obligado contará con un Comité de Transparencia colegiado, mismo que adoptará sus resoluciones por mayoría de votos.

El nueve de mayo de dos mil dieciséis, se publicó en el Diario Oficial de la Federación la (LFTAIP), misma que en su artículo 64 establece que, los Comités de Transparencia se integrarán por el responsable del Área Coordinadora de Archivos;

PARTICULAR, SON REGLADAS Y NO DISCRECIONALES. Tesis: I.4o.A.211 A (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. III, febrero de 2021, p. 2867.

[263] JUICIO CONTENCIOSO ADMINISTRATIVO FEDERAL. ES IMPROCEDENTE CONTRA LAS RESOLUCIONES EMITIDAS POR EL INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES (INAI), EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE PARTICULARES. Tesis: 2a./J. 31/2020 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. I, octubre de 2020, p. 668.

el Titular de la Unidad de Transparencia y el Titular del Órgano Interno de Control.

El Comité de Transparencia tendrá como objetivo instruir, coordinar y supervisar las acciones en materia de transparencia, acceso a la información pública y protección de datos personales que lleve a cabo la Unidad de Transparencia y las unidades administrativas de los sujetos obligados, a fin de garantizar la transparencia, el acceso a la información y la protección de los datos personales que se encuentran bajo su custodia, en términos de la Ley General de Transparencia y Acceso a la Información Pública, la Ley Federal de Transparencia y Acceso a la Información Pública y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Otras obligaciones que tienen son los siguientes:

			
Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho de transparencia y rendición de cuentas en los sujetos obligados.	Instituir procedimientos internos para asegurar la mayor en las solicitudes de Transparencia.	Sesionar para determinar la inexistencia de información.	Clasificar y desclasificar la Información.
			
Integrar la Información en el SIPOT.	Dar cumplimiento a las resoluciones de los Organismos Garantes.	Establecer programas de capacitación y actualización para los servidores públicos en el sujeto obligado.	En su caso, informar al Organo Interno de Control de presuntas irregularidades de los servidores públicos en la materia.

El artículo 57 último párrafo del Reglamento de la LFTAIP dispone que cada Comité establecerá los criterios para su funcionamiento, los cuales deberán prever al menos la periodicidad con que sesionará, el servidor público que lo presidirá y la forma de

dar seguimiento a sus acuerdos. Algunos sujetos obligados tienen reglamentos en lugar de lineamientos de funcionamiento.

Cabe señalar que cada sujeto obligado tiene publicados sus lineamientos o reglamentos con características propias, además de las obligaciones de ley.

3.3.5. Unidades de Transparencia.

Se podría decir válidamente, que las unidades de transparencia son la cara de entrada en el ejercicio del derecho de acceso a la información. Constituyen la instancia (oficina) del sujeto obligado, encargada de publicar la información fundamental, así responder, en tiempo y forma, a las solicitudes de información.

Estas unidades de transparencia también son denominadas unidades de enlace. Las funciones principales en materia de transparencia y acceso a la información son las siguientes:

1) Auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho a la Información.
2) Gestionar las solicitudes para el ejercicio de acceso a la información.
3) Establecer mecanismos para asegurar que se entregue la información solicitada.
4) Informar al peticionario o su representante el monto de los costos a cubrir por la reproducción y envío de la información en su caso.
5) Proponer al Comité de Transparencia los procedimientos internos que aseguren y fortalezcan mayor eficiencia en la gestión de las solicitudes de transparencia y acceso a la información.
6) Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes de transparencia y acceso a la información.
7) Asesorar a las áreas adscritas al responsable en materia de acceso a la información.

Cabe mencionar que esta Unidad de Transparencia también cuenta con atribuciones en materia de datos personales, las cuales serán descritas en el apartado respectivo.

Estas unidades de transparencia también son denominadas unidades de enlace; lo anterior, es importante advertirlo porque no son una instancia resolutoria, sino que "sus facultades se limitan a servir como vínculo entre la dependencia o entidad y el solicitante de información, y no así para emitir resoluciones terminales, ya que tal facultad corresponde al Comité respectivo."[264]

[264] RECURSO DE REVISIÓN PREVISTO EN EL ARTÍCULO 49 DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL. ES IMPROCEDENTE CONTRA LAS RESOLUCIONES EMITIDAS POR LA UNIDAD DE ENLACE DE LA COMISIÓN FEDERAL DE TELECOMUNICACIONES EN LAS QUE COMUNICA SOBRE LA CLASIFICACIÓN DE INFORMACIÓN. Tesis: 2a./J. 137/2015 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. II, octubre de 2015, p. 1976.

Ahora bien, cuando se reclame la respuesta emitida por el titular de la Unidad Especializada de Transparencia y Apertura Gubernamental de la Procuraduría General de la República, en un procedimiento administrativo de acceso a la información, previsto en la Ley Federal de Transparencia y Acceso a la Información Pública, será competencia de los Jueces de Distrito de Amparo en Materia Penal, si la respuesta contiene la interpretación de normas que corresponden al ámbito de la pretensión punitiva del Estado, pues si bien el artículo 61, fracciones I, II y IV, de esta última ley prevé que la unidad de transparencia respectiva tiene como funciones la de recibir y dar trámite a las solicitudes de acceso a la información, coordinar su difusión, así como realizar los trámites internos necesarios para la atención de las solicitudes de acceso a la información, entre otras; estas funciones no justifican, *per se*, que el juicio de amparo indirecto sea de la competencia en materia penal y/o administrativa, pues ello deberá vincularse con el contenido de la respuesta que se dé a la petición de información; de ahí que si se promueve un juicio de amparo indirecto contra la respuesta vinculada con la solicitud de información relacionada con una investigación criminal, averiguación previa o carpeta de investigación, en la que, para darla, hay que atender a la operatividad de normas penales, el conocimiento del juicio de amparo, conforme al artículo 51 mencionado, corresponde a un Juez de Distrito de Amparo en Materia Penal.[265]

El ejercicio de las atribuciones de la unidad de transparencia han sido interpretadas por los tribunales en las siguientes tesis:

- Pruebas en el amparo indirecto. No existe obligación del juzgador de requerir las copias o documentos ofrecidos y solicitados en términos de la ley federal de transparencia y acceso a la información pública a una unidad de enlace o unidad de transparencia, aun cuando en la petición se haya invocado el artículo 121 de la ley de amparo.[266]
- Pruebas en el juicio de amparo indirecto. Si una de las partes ofrece copias o documentos en poder de una autoridad, los cuales solicitó sin que se expidieran, el juez de distrito, de conformidad con el artículo 121 de la ley de la materia, debe requerírselos, aun cuando la petición a esa autoridad se haya efectuado a través de su unidad de enlace o de transparencia, en términos de la ley federal de transparencia y acceso a la información pública.[267]

[265] COMPETENCIA POR MATERIA PARA CONOCER DEL AMPARO PROMOVIDO CONTRA LA RESPUESTA DEL TITULAR DE LA UNIDAD ESPECIALIZADA DE TRANSPARENCIA Y APERTURA GUBERNAMENTAL DE LA PROCURADURÍA GENERAL DE LA REPÚBLICA A UNA SOLICITUD DE ACCESO A LA INFORMACIÓN RELACIONADA CON UNA INVESTIGACIÓN CRIMINAL, AVERIGUACIÓN PREVIA O CARPETA DE INVESTIGACIÓN. SI LA CONTESTACIÓN CONTIENE LA INTERPRETACIÓN DE NORMAS PENALES, CORRESPONDE A UN JUZGADO DE DISTRITO DE AMPARO EN MATERIA PENAL. Tesis: I.6o.P.130 P (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. II, diciembre de 2018, p. 1071.

[266] Tesis: I.1o.A.E.42 K (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. IV, enero de 2016, p. 3397.

[267] Tesis: III.5o.A.3 K (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. IV,

De estas tesis derivó la siguiente Jurisprudencia:

> PRUEBA DOCUMENTAL EN EL JUICIO DE AMPARO. EN TÉRMINOS DEL ARTÍCULO 121 DE LA LEY DE AMPARO, EL SERVIDOR PÚBLICO QUE POSEA ALGÚN DOCUMENTO OFRECIDO Y ADMITIDO COMO TAL NO PUEDE REHUSARSE A UN REQUERIMIENTO JUDICIAL, SOBRE LA BASE DE QUE DEBE ESTARSE A LO RESUELTO EN UN PROCEDIMIENTO DE ACCESO A LA INFORMACIÓN.[268]
> En términos del precepto citado, y conforme a los derechos de audiencia y de plenitud en la impartición de justicia, el órgano jurisdiccional de amparo debe requerir a cualquier servidor público la exhibición de un documento ofrecido y admitido como prueba conforme a derecho, en cuyo caso, el servidor público que lo posea no puede oponerse a ello, argumentando que existe un impedimento jurídico, en virtud de que la información contenida en el documento debe sujetarse a un procedimiento de transparencia, que está sujeto a un procedimiento de esta naturaleza pendiente de resolución, o incluso que fue objeto de una resolución por parte del organismo garante o de alguno de los organismos especializados locales en materia de acceso a la información pública, en la que se determinó que el documento contiene datos clasificados como confidenciales o reservados; lo anterior, pues la exhibición del documento en el juicio de amparo no implica ni permite que esos datos se publiquen o divulguen ya que, en primer término, el público en general sólo tendrá acceso, en su caso, a una versión pública en la que esos datos se supriman y, en segundo lugar, el órgano jurisdiccional únicamente podrá permitir a las partes el acceso a dichos datos, bajo su más estricta responsabilidad: (i) si su valoración es precisamente la prueba idónea respecto de los hechos a demostrar, siempre que el objeto del acto reclamado no sea el acceso a esa información; (ii) si ello es indispensable para que una o algunas de las partes hagan valer sus derechos con la pretensión de que se dicte una resolución apegada a derecho, bajo su responsabilidad en cuanto al uso y destino de dichos datos; y (iii) con las condiciones y medidas que el propio juzgador considere necesarias para la protección de los datos de que se trata.

3.3.6. Consejo Consultivo

El Consejo Consultivo es un órgano plural, honorífico y ciudadano creado por disposición constitucional, que participa de forma conjunta y coordinada en la promoción de los derechos de acceso a la información pública y de protección de datos personales, fortaleciendo las funciones del INAI y su relación con la sociedad.

La integración del Consejo Consultivo garantiza la igualdad de género y la inclusión de personas con experiencia en las materias de transparencia, acceso a la información pública, protección de datos personales y, en general, de los derechos humanos.

---

septiembre de 2016, p. 2890.

[268] Tesis: P./J. 13/2018 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. I, junio de 2018, p. 12.

En términos del artículo 6º, apartado A, de la Constitución Política de los Estados Unidos Mexicanos, se integra por diez consejeros honoríficos provenientes de las organizaciones de la sociedad civil y la academia, nombrados por el Senado de la República después de una convocatoria pública dirigida a instituciones académicas, de investigación, asociaciones, colegios de profesionales y la sociedad en general.

El Consejo funciona en sesiones ordinarias y extraordinarias, tomando sus decisiones por mayoría de votos, de conformidad con lo dispuesto por la Ley Federal de Transparencia y Acceso a la Información Pública, el Estatuto Orgánico del Instituto y sus propias Reglas de Operación.

La Ley Federal de Transparencia y Acceso a la Información Pública establece que el Consejo Consultivo del INAI tiene las atribuciones siguientes:

1) Aprobar sus reglas de operación.
2) Presentar al Pleno su informe anual de actividades.
3) Opinar sobre el programa anual de trabajo del Instituto y su cumplimiento.
4) Emitir un informe anual sobre el desempeño del Instituto.
5) Opinar sobre el proyecto de presupuesto para el ejercicio del año siguiente.
6) Conocer el informe del Instituto sobre el presupuesto asignado a programas y el ejercicio presupuestal y emitir las observaciones correspondientes.
7) Emitir opiniones no vinculantes al Instituto sobre temas relevantes en las materias de transparencia, acceso a la información, accesibilidad y protección de datos personales.
8) Emitir opiniones técnicas para la mejora continua en el ejercicio de las funciones sustantivas del Instituto.
9) Opinar sobre la adopción de criterios generales en materia sustantiva.
10) Proponer mejores prácticas de participación ciudadana y colaboración en la implementación y evaluación de la regulación en materia de datos abiertos.
11) Analizar y proponer la ejecución de programas, proyectos y acciones relacionadas con la materia de transparencia y acceso a la información y su accesibilidad.
12) Las que deriven de la Ley General y esta Ley. Las opiniones emitidas por el Consejo Consultivo referidas en el presente artículo serán públicas.

Además de la Ley Federal de Transparencia este consejo cuenta con reglas de operación, las cuales tienen por objeto establecer las normas internas de integración, estructura y funcionamiento del Consejo Consultivo del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

La importancia del Consejo Consultivo radica en que -con su labor- contribuye a consolidar la cultura de la rendición de cuentas en el país, así como a velar por el respeto del derecho fundamental a contar con información fidedigna y oportuna, como llave de acceso al ejercicio de nuevos derechos ciudadanos.

Además, su papel es relevante, dado que -desde un punto de vista técnico- se instituye como la principal fuente consultiva a la que el INAI puede acudir en aquellos casos controversiales o de trascendencia pública.

En ese contexto, si bien la existencia del Consejo Consultivo ha sido breve, lo cierto es que después de cuatro años de vida institucional, su labor muestra que ha generado mayores espacios de comunicación entre la sociedad civil y el INAI, tendiendo puentes de reflexión, diálogo, análisis y propuestas plurales que son necesarias en un estado democrático.[269]

Las opiniones sobre las que se ha pronunciado son las siguientes:[270]

2021

- Opinión relativa a la protección de datos personales en el registro de vacunación contra COVID-19.
- Opinión relativa a la reforma sobre la creación del Padrón Nacional de Usuarios Móviles.
- Opinión relativa al anteproyecto de presupuesto 2022 del INAI
- Opinión relativa al proyecto del Programa Institucional 2021-2024 del INAI
- Opinión relativa al hackeo de la Plataforma Nacional de Transparencia
- Opinión relativa a la evaluación de impacto con las reformas del CFF
- Opinión relativa al Acuerdo que determina como seguridad nacional obras de infraestructura

2020

- Opinión relativa a la necesidad de realizar evaluación de impacto sobre intención de transferencia de datos personales.
- Opinión relativa a la publicación de infografías sobre resoluciones relevantes del INAI.
- Opinión sobre la suspensión de plazos del INAI (COVID-19).
- Opinión sobre el comunicado de las OSC por suspensión de plazos del INAI (COVID-19)
- Opinión relativa al anteproyecto de presupuesto 2021 del INAI

2019

- Opinión relativa a transparentar la atención brindada a las resoluciones del INAI.
- Opinión relativa a las disposiciones de compensación de los servidores públicos de carrera de la APF.

---

[269] Gutiérrez Salazar, Miguel Ángel, *El Consejo Consultivo del INAI: Retos Presentes y Futuros | 2021*, [en línea] México, Rendición de cuentas.org, Secc. Opinión, octubre 12, 2021, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.rendiciondecuentas.org.mx/el-consejo-consultivo-del-inai-retos-presentes-y-futuros/*

[270] El texto completo de cada una de las opiniones se puede ver en los hipervínculos de la página del Consejo Consultivo del INAI,
https://proyectos.inai.org.mx/consejoconsultivo/index.php/actividades/opiniones

- Opinión relativa a la inclusión de la figura de la conciliación en los recursos de revisión en materia de acceso a la información pública.
- Opinión en materia de mejora regulatoria.
- Opinión relativa a terceros interesados y documentos fuente tratándose de solicitudes relacionadas con información comentada en conferencias de prensa
- Opinión relativa al anteproyecto de presupuesto 2020 del INAI

2018

- Opinión sobre el Programa Anual de Trabajo 2018 del INAI.
- Opinión sobre la Ley de Seguridad Interior.
- Opinión sobre la actualización del enlace de vacantes en el portal del INAI.
- Opinión relativa a establecer un régimen de incompatibilidades temporales para los Comisionados del INAI.
- Opinión relativa a no solicitar la presencia física para participar en convocatorias al CC-INAI y al Pleno del INAI
- Opinión relativa a la transparencia del currículo de los candidatos.
- Opinión relativa a la integración de los Consejos Consultivos por servidores públicos.
- Opinión acerca del Plan Nacional de Socialización del Derecho de Acceso a la Información.
- Opinión sobre el anteproyecto del Presupuesto 2019 del INAI.

2017

- Opinión sobre el anteproyecto de Presupuesto 2018 del INAI.
- Opinión sobre el tema de Espionaje y la garantía del derecho humano a la protección de los datos personales.
- Opinión sobre la pertinencia de premiar por el cumplimiento de las obligaciones de transparencia.
- Opinión sobre la incorporación dentro del trabajo editorial del INAI de una nueva serie o línea editorial que destaque el debate y discusiones, contemporáneas.
- Opinión sobre el reconocimiento de buenas prácticas de apertura gubernamental por parte del INAI.
- Opinión relativa a garantizar la transparencia en el ejercicio de los recursos destinados a los Fondos para la Reconstrucción de la Vivienda.
- Opinión sobre el proyecto del Programa Institucional 2017-2020 del INAI.
- Opinión sobre la propuesta del Programa Nacional de Transparencia y Acceso a la Información (PROTAI) 2017-2021.
- Opinión sobre la necesidad de proteger los datos personales sensibles que se registran en la aplicación móvil utilizada para la captación de apoyo ciudadano, a través de la cual los aspirantes a cargos federales de elección popular deben registrar dicho apoyo con miras a obtener su registro como candidatos independientes.
- Opinión sobre el proyecto de la Ley de Seguridad Interior.

3.4. Plataforma Nacional de Transparencia

La Plataforma Nacional de Transparencia (PNT) constituye actualmente el medio uniforme por medio del cual se realizan las acciones de acceso a la información y protección de datos personales en posesión de sujetos obligados; sin embargo, esto no siempre fue así.

La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental entró en vigor el 12 de junio de 2002, y que en su artículo octavo transitorio estableció que los particulares podrían presentar las solicitudes de acceso a la información, a los datos personales y a la corrección de éstos un año después.

En aquel entonces se tuvieron 33 leyes de acceso a la información con procedimientos diferentes para atender solicitudes de acceso a la información pública y se sabe que algunas instituciones desarrollaron su propio sistema para gestionar solicitudes.

Fue por ello que a partir del 12 de junio de 2003, adicionalmente a la posibilidad de presentar solicitudes de acceso a la información, y de acceso y corrección de los datos personales, a través de los formatos autorizados por el entonces IFAI, se creó un sistema electrónico denominado Sistema de Solicitudes de Información (SISI), con el propósito de facilitar el ejercicio del derecho de acceso a la información, así como el de acceso y corrección de datos personales, a tal efecto, el Instituto Federal de Acceso a la Información Pública, publicó los Lineamientos respectivos en el Diario Oficial de la Federación, con fechas 12 de junio y 25 de agosto de 2003, así como 6 de abril de 2004.

Dichos lineamientos tenían por objeto establecer las reglas que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento y trámite de las solicitudes de acceso a la información gubernamental, que formulen los particulares, así como en su resolución y notificación, y la entrega de la información en su caso, con exclusión de las solicitudes de acceso a datos personales y su corrección.
El sistema SISI estaba definido de la siguiente forma:

> Segundo. Además de las definiciones contenidas en los artículos 3 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, y 2 de su Reglamento, para los efectos de los presentes Lineamientos se entenderá por:
> I. Sistema de Solicitudes de Información o SISI: el sistema autorizado por el Instituto que contiene los formatos impresos y electrónicos para que las personas presenten sus solicitudes de acceso a través de medios electrónicos, y el sistema único para el registro y captura de todas las solicitudes recibidas por las dependencias y entidades en otros medios como correo, mensajería o físicamente, y cuyo sitio de Internet es http://informacionpublica.gob.mx;

Con la reforma del 20 de julio de 2007, publicado en el Diario Oficial de la Federación el decreto por el que se adiciona un segundo párrafo con siete fracciones al artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, en el que se reconoció expresamente el derecho de acceso a la información como un derecho fundamental y se establecieron los principios y bases que deben regir, en el orden federal, estatal y municipal, en el ejercicio de este derecho; el artículo tercero transitorio del decreto de referencia, prevé que la Federación, los Estados y el Distrito Federal deberán contar con sistemas electrónicos para que cualquier persona pueda hacer uso remoto de los mecanismos de acceso a la información, a sus datos personales y la rectificación de los mismos, así como de los procedimientos de revisión, a más tardar en dos años a partir de la entrada en vigor del mismo.

Por lo anterior, para estandarizar el uso de medios electrónicos y homogeneizar los mecanismos para presentar solicitudes de acceso a la información, y de acceso y rectificación de datos personales, así como recursos de revisión, se hizo necesario que en la Administración Pública Federal, en sustitución del Sistema de Solicitudes de Información (SISI), se implementara el Sistema INFOMEX, a efecto de que los particulares cuenten con el mismo sistema informático en los diversos sujetos obligados por la Ley, así como en las entidades federativas en las que se ha adoptado dicho Sistema.

El cambio de un sistema a otro no representó ningún costo adicional a los particulares que ya se encontraban registrados en el SISI, toda vez que el Sistema INFOMEX reconocerá los nombres de usuario y contraseñas que éstos venían utilizando; sin embargo, fue necesario modificar los Lineamientos que expidió el IFAI en relación con el Sistema de Solicitudes de Información, lo que ocurrió el 02 de diciembre de 2008 cuando se publicaron las Modificaciones a los Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento y trámite de las solicitudes de acceso a la información gubernamental que formulen los particulares, así como en su resolución y notificación, y la entrega de la información en su caso, con exclusión de las solicitudes de acceso a datos personales y su corrección; Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de acceso a datos personales que formulen los particulares, con exclusión de las solicitudes de corrección de dichos datos, y Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal, en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de corrección de datos personales que formulen los particulares.

En estas modificaciones, el sistema INFOMEX se definió de la siguiente manera:

> I. Sistema INFOMEX: el sistema autorizado por el Instituto que contiene los formatos impresos y electrónicos para que las personas presenten sus solicitudes de acceso a través de medios

> electrónicos, y el sistema único para el registro y captura de todas las solicitudes recibidas por las dependencias y entidades en otros medios como correo, mensajería o físicamente, y cuyo sitio de Internet es www.infomex.org.mx/gobiernofederal;

En este sentido el INFOMEX se convirtió en una especie de plataforma común que sirvió para gestionar las solicitudes de información y atención de recursos de revisión a todo el Ejecutivo Federal, otros organismos constitucionales autónomos, los otros dos poderes federales, entidades federativas y municipios, así como tribunales federales.

La Plataforma del INFOMEX estuvo funcionando por 14 años hasta el denominado "Día Cero", que consistió en que el 11 y 12 de septiembre de 2021 se llevó a cabo la suspensión provisional de la Plataforma Nacional de Transparencia, la migración de solicitudes del sistema INFOMEX y la realización de pruebas para óptimo funcionamiento. El día 13 de septiembre de 2021 se dio inicio de operaciones al denominado SISAI 2.0 y el reinicio de la PNT.

Con la expedición de la nueva Ley General de Transparencia, publicada en el DOF del 04 de mayo de 2015 el artículo 61 menciona que los lineamientos técnicos que emita el Sistema Nacional establecerán los formatos de publicación de la información para asegurar que la información sea veraz, confiable, oportuna, congruente, integral, actualizada, accesible, comprensible, verificable.

Por lo anterior, el 04 de mayo de 2016 se publicaron en el DOF el Acuerdo del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, por el que se aprueban los Lineamientos para la implementación y operación de la Plataforma Nacional de Transparencia.

Dichos lineamientos tienen por objeto establecer las reglas de operación de la Plataforma Nacional de Transparencia, que garanticen su estabilidad y seguridad, promoviendo la homologación de procesos y la simplicidad del uso de los sistemas que conforman dicha Plataforma para los usuarios, garantizando en todo momento los derechos de acceso a la información y protección de datos personales en posesión de los sujetos obligados.
La Plataforma Nacional es el instrumento informático a través del cual se ejercerán los derechos de acceso a la información y de protección de datos personales en posesión de los sujetos obligados, así como su tutela, en medios electrónicos, de manera que garantice su uniformidad respecto de cualquier sujeto obligado, y sea el repositorio de información obligatoria de transparencia nacional.

Los organismos garantes desarrollarán, administrarán, implementarán y pondrán en funcionamiento la Plataforma Nacional que permita cumplir con los procedimientos, obligaciones y disposiciones señaladas en la Ley General para los sujetos obligados y organismos garantes, de conformidad con la normatividad que establezca el Sistema Nacional, atendiendo a las necesidades de accesibilidad de los usuarios.

La Plataforma Nacional estará conformada por, al menos, los siguientes sistemas:

I. Sistema de Solicitudes de Acceso a la Información (SISAI);
II. Sistema de Gestión de Medios de Impugnación (SIGEMI);
III. Sistema de Portales de Obligaciones de Transparencia (SIPOT), y
IV. Sistema de Comunicación entre Organismos Garantes y Sujetos Obligados (SICOM).

Las solicitudes correspondientes al ejercicio de los derechos ARCOP[271], serán tramitadas por medio de la Plataforma Nacional o el sistema local implementado, conforme a la legislación aplicable.

En 2021 se puso en marcha el Sistema de Solicitudes de Acceso a la Información en su nueva versión (SISAI 2.0), que comprende una serie de funcionalidades que mejoran su experiencia operativa, tanto para el solicitante como para los sujetos obligados. Un logro destacado es que se migraron las solicitudes de información de los 32 sistemas INFOMEX estatales y el sistema federal a la PNT, agrupando en un solo sitio su historial, que ahora está inscrito en la PNT. En esta versión también se incluyó el derecho de portabilidad de datos personales.[272]

3.5 Obligaciones de Transparencia

Uno de los títulos más importantes de la Ley General es el relativo a las obligaciones de transparencia, en el cual se establece la divulgación por Internet de información de interés general para todas las personas, cuyo acceso no dependa de una solicitud expresa, lo que habilita la apertura informativa de los sujetos obligados.

De tal manera, dichos sujetos obligados deberán poner a disposición la información pública de interés general, en formatos abiertos, en sus respectivos sitios de Internet y a través de la Plataforma Nacional de Transparencia.
La información deberá actualizarse por lo menos cada tres meses de manera general, y ser veraz, confiable, oportuna, gratuita, congruente, integral, accesible, comprensible y verificable. Deberá publicarse con perspectiva de género y discapacidad, cuando así corresponda a su naturaleza, procurando su accesibilidad de manera focalizada a personas que hablen alguna lengua indígena.

La Ley General incluye el catálogo de información considerada como pública de oficio y que deben publicar los Sujetos Obligados en sus portales de INTERNET y en la Plataforma, mismo que se complementa con la información específica que deben publicar el órgano ejecutivo, legislativo, judicial, órganos políticos administrativos, alcaldías o demarcaciones territoriales, autoridades electorales,

[271] Acceso, Rectificación, Cancelación, Oposición y Portabilidad.
[272] De Jesús Lozano Ocman, Magda Eugenia, *Propuesta de Plan de Trabajo 2021-2022 para la Coordinación de la Comisión de Tecnologías de la Información y Plataforma Nacional de Transparencia*, [en línea] México, SNT-INAI, 2021, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://snt.org.mx/wp-content/uploads/2022/01/MEJLO_TIyPNT_2022.pdf* p. 1.

fideicomisos y fondos, organizaciones políticas, Órganos Constitucionales Autónomos y sindicatos, así como de las obligaciones específicas de las personas físicas o morales que reciban y ejerzan recursos públicos o actos de autoridad.

La Ley General establece en su artículo 70 (setenta) un catálogo de obligaciones de transparencia comunes, o información pública de oficio; la cual, deberán publicar de manera obligatoria todos los sujetos obligados, siendo algunas de ellas las siguientes:

- Marco normativo aplicable;
- Directorio, estructura orgánica, facultades y funciones de cada área;
- Metas, objetivos y resultados de cada área conforme a sus programas operativos, incluyendo indicadores para la rendición de cuentas;
- Remuneraciones, viáticos y gastos de representación de todos los servidores públicos;
- Contrataciones de servicios profesionales por honorarios;
- Información curricular y perfil de puesto de las personas servidoras públicas;
- Versión pública de las Declaraciones Patrimoniales, de Intereses y Fiscal de las personas servidoras públicas y colaboradores de los Sujetos Obligados;
- Listado de personas servidoras públicas con sanciones administrativas definitivas;
- Información financiera sobre el presupuesto asignado y su ejecución;
- Programas operativos anuales y de trabajo;
- Informes de resultados de auditorías al ejercicio presupuestal;
- Concesiones, contratos, convenios, permisos, licencias, y autorizaciones
- Información de los resultados sobre procedimientos de adjudicación directa, invitación restringida y licitación de cualquier naturaleza;
- Informes de avances programáticos o presupuestales;
- Mecanismos de participación ciudadana;
- Catálogo de disposición y guía de archivo documental;

El artículo 67 de la Ley General establece que la información publicada por los Sujetos Obligados, en términos de sus obligaciones de transparencia, no constituye propaganda gubernamental, por lo que durante los procesos electorales (a partir del inicio de las precampañas y hasta la conclusión del proceso electoral), los Sujetos Obligados deberán mantener accesible la información de oficio en sus portales de obligaciones de transparencia, salvo disposición expresa en contrario en la normatividad electoral.

Cabe advertir, que las obligaciones de transparencia, no llegan a ser del todo claras, sobre todo en el caso de los sindicatos; por ello la SCJN, emitió la siguiente jurisprudencia:

> SINDICATOS, FEDERACIONES Y CONFEDERACIONES. EL ARTÍCULO 358, FRACCIÓN IV, DE LA LEY FEDERAL DEL TRABAJO, AL ESTABLECER EL DEBER DE SU DIRECTIVA DE RENDIR CUENTA COMPLETA Y DETALLADA DE LA ADMINISTRACIÓN DE SU

PATRIMONIO, NO VIOLA EL DERECHO DE ACCESO A LA INFORMACIÓN Y DE PROTECCIÓN DE DATOS PERSONALES (LEGISLACIÓN VIGENTE A PARTIR DEL 1 DE MAYO DE 2019).
Hechos: Varios sindicatos promovieron juicios de amparo indirecto en contra del artículo 358, fracción IV, de la Ley Federal del Trabajo, reformado mediante decreto publicado en el Diario Oficial de la Federación el 1 de mayo de 2019, al considerar que la obligación impuesta a la directiva sindical de rendir cuenta completa y detallada de la administración de su patrimonio a sus agremiados, implica una violación al derecho de salvaguardar los datos personales de la asociación sindical, de conformidad con el artículo 6o., apartado A, de la Constitución Política de los Estados Unidos Mexicanos.
Criterio jurídico: La Segunda Sala de la Suprema Corte de Justicia de la Nación determina que la obligación impuesta a las directivas sindicales en el artículo 358, fracción IV, de la Ley Federal del Trabajo, de rendir cuenta completa y detallada de la administración de los recursos del sindicato, no vulnera el derecho de acceso a la información y protección de datos personales.
Justificación: De acuerdo con los artículos 6o., apartado A, 16, párrafo segundo y 123, apartado A, fracciones XVI y XXII Bis, de la Constitución Política de los Estados Unidos Mexicanos, los trabajadores que decidan asociarse en sindicatos tienen derecho a la protección de sus datos personales en posesión de particulares o de cualquier autoridad. De esa manera, las directivas de los sindicatos, federaciones y confederaciones, al cumplir con su deber de rendir cuenta a sus agremiados, deben actuar en términos de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, la cual establece el tratamiento que un particular debe dar a la información personal en posesión de particulares, cuyo fin es garantizar la privacidad y el derecho de autodeterminación informativa de las personas, lo que no vulnera el derecho de acceso a la información y protección de datos personales, pues parte del principio de representatividad de sus agremiados es precisamente brindarles información del patrimonio del sindicato y su administración, por ser quienes lo integran y aportan sus cuotas.[273]

Otro sujeto obligado de naturaleza híbrida [privado-público] son las asociaciones deportivas nacionales, también llamadas federaciones deportivas, ejercen, por delegación, funciones públicas de carácter administrativo, actuando como agentes colaboradores del Gobierno Federal, por lo que dicha actuación se considerará de utilidad pública.

En este sentido, algunas federaciones deportivas reciben recursos públicos para eventos deportivos, becas para algunos deportistas entre otras actividades; por ello también se les debe considerar sujetos obligados para efectos de Transparencia y Acceso a la Información. Sirve para lo anterior la siguiente tesis:

[273] Tesis: 2a./J. 10/2021 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. II, marzo de 2021, p. 1651.

FEDERACIONES DEPORTIVAS MEXICANAS. SON SUJETOS DE FISCALIZACIÓN Y QUEDAN VINCULADAS POR LOS DERECHOS A LA LIBERTAD DE EXPRESIÓN Y DE ACCESO A LA INFORMACIÓN.
Al manejar recursos públicos, las Federaciones Deportivas Mexicanas cuentan con distintas obligaciones previstas constitucional y legalmente, por lo que son sujetos de fiscalización y, por ende, de escrutinio en cuanto al manejo de los recursos destinados a los propósitos que fijen las leyes correspondientes, esto es, que todos los actos encaminados a la custodia y cuidado de los recursos públicos se cumplan cabalmente, se vigile, investigue y compruebe de la mejor manera la existencia de posibles conductas ilícitas que atenten contra los valores y funciones mencionadas y, en su caso, que se impongan las sanciones establecidas para ese efecto en las leyes respectivas, con base en los procedimientos administrativos sancionadores correspondientes. Lo anterior, a efecto de evitar que cualquier entidad, incluyendo cualquier persona moral privada que maneje recursos públicos federales, quede fuera de control y de la rendición de cuentas, para corroborar la aplicación adecuada y su uso correcto. Por otra parte, los derechos a la libertad de expresión y de acceso a la información no sólo protegen libertades necesarias para la autonomía personal de los individuos, sino también pretenden proteger y garantizar un espacio público de deliberación política; por tanto, la libertad de expresión y el acceso a la información tienen una doble dimensión: una personal y otra colectiva, siendo la última un bien público de naturaleza constitucional, que se debe preservar y perfeccionar. Así, mientras existan mejores condiciones para el ejercicio desinhibido de las libertades de expresión y de acceso a la información, también las habrá por el de los derechos políticos indispensables para el funcionamiento de la democracia representativa. En consecuencia, se trata de un derecho que, al ser ejercido ante una entidad de la administración pública o de cualquier ente que esté regido por la obligación de transparencia y rendición de cuentas, genera un interés jurídico por la omisión de no recibir respuesta en relación con la información solicitada, con independencia de que pueda o no ser clasificada como reservada y que en el fondo no se tenga la obligación de expedir; de ahí que las Federaciones Deportivas Mexicanas estén vinculadas por los derechos a la libertad de expresión y de acceso a la información.[274]

Por lo anteriormente planteado, a juicio del que esto escribe, de manera general, se puede señalar que los sujetos obligados a que hace mención el artículo sexto constitucional, son los siguientes:

Gobierno Central

Poder Legislativo

Poder Judicial

[274] Tesis: PC.I.A. 2 A (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. III, agosto de 2016, p. 2253.

Desconcentrados, descentralizados, paraestatales y auxiliares

Entidades Federativas, Municipios y Alcaldías

Fondos y fideicomisos

Organismos Autónomos

Partidos Políticos

Sindicatos

Personas físicas o morales

Asimismo, en el Diario Oficial de la Federación, se publica una relación de sujetos obligados en el ámbito federal. Sobre el particular, se han publicado los siguientes acuerdos:

Fecha de Publicación en el DOF	Nombre del Acuerdo
04/05/2016	ACUERDO mediante el cual el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, aprueba el padrón de sujetos obligados del ámbito federal, en términos de la Ley General de Transparencia y Acceso a la Información Pública.
29/08/2019	ACUERDO mediante el cual se aprueba que el padrón de sujetos obligados del ámbito federal, en términos de la Ley General de Transparencia y Acceso a la Información Pública y sus respectivas actualizaciones llevadas a cabo por la Secretaría de Acceso a la Información, se utilice como referencia directa del catálogo de sujetos obligados en el ámbito federal para efectos de lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
04/06/2021	ACUERDO mediante el cual se aprueba la actualización del Padrón de personas físicas y morales que recibieron y ejercieron recursos públicos o que fueron facultados para realizar actos de autoridad, durante el ejercicio fiscal dos mil veinte, y se determina la forma en que deberán cumplir con sus obligaciones de transparencia y acceso a la información.

Importante señalar también que, además de las 48 obligaciones comunes de transparencia; en los artículos 71 a 83 de la LGTAIP, se señalan otras obligaciones, las cuales aplican a diferentes sujetos obligados, constituyendo las "obligaciones de transparencia específicas"

En este sentido, el pasado 04 de mayo de 2016, fueron publicadas en el DOF, el Acuerdo del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, por el que se aprueban los Lineamientos técnicos generales para la publicación, homologación y estandarización de la información de las obligaciones establecidas en el título quinto y en la fracción IV del artículo 31 de la Ley General de Transparencia y Acceso a la Información Pública, que deben de difundir los sujetos obligados en los portales de Internet y en la Plataforma Nacional de Transparencia.

Este acuerdo define lo que debe entenderse como obligaciones comunes y obligaciones específicas de transparencia en los siguientes términos:

> Segundo. Para los efectos de los presentes Lineamientos, se entenderá por:
> XV. Obligaciones comunes: Son aquellas que describen la información que deberán poner a disposición de los particulares y mantener actualizada en los sitios de Internet correspondientes y en la Plataforma Nacional todos los sujetos obligados, sin excepción alguna, y que se refieren a temas, documentos y políticas que aquellos poseen en ejercicio de sus facultades, obligaciones y el uso de recursos públicos, respecto de: su organización interna y funcionamiento, atención al público, ejercicio de los recursos públicos, determinaciones institucionales, estudios, ingresos recibidos y donaciones realizadas, organización de archivos, entre otros;
> XVI. Obligaciones específicas: Constituyen la información que producen sólo determinados sujetos obligados a partir de su figura legal, atribuciones, facultades y/o su objeto social;

La importancia de este acuerdo es la siguiente:

1. Establece las pautas para la organización, difusión y actualización de la información derivada de las obligaciones de transparencia comunes y específicas de los sujetos obligados.
2. Define las características de la información que menciona el artículo 61 de la LGTAI (veraz, confiable, oportuna, congruente, integral, actualizada, accesible, comprensible, verificable)
3. Indica las políticas para actualizar la información de los sujetos obligados.
4. Menciona las políticas de aplicabilidad.
5. Detalla las políticas para la distribución de competencias y responsabilidades para la carga de la información prescrita en el Título Quinto de la Ley General.
6. Dispone las políticas para la verificación y vigilancia de la información.
7. Coloca las políticas para accesibilidad de la información.

8. Se detallan y puntualizan por medio de diferentes anexos, los criterios sustantivos y adjetivos que por cada rubro de información determinan los datos, características y forma de organización de la información que publicarán y actualizarán en sus portales de Internet y en la Plataforma Nacional, los sujetos obligados de acuerdo con su naturaleza jurídica y misión institucional en los distintos ámbitos: federal, estatal, municipal y delegacional.

La información que se debe cumplimentar de acuerdo con los diferentes Anexos es la siguiente:

Anexo 1 se detallan los criterios sustantivos y adjetivos que por cada rubro de información determinan los datos, características y forma de organización de la información que publicarán y actualizarán en sus portales de Internet y en la Plataforma Nacional, todos los sujetos obligados en los distintos ámbitos: federal, estatal, municipal y delegacional, de conformidad con lo establecido en el artículo 70.
Anexo 2: artículo 71, Poderes Ejecutivos Federal, de las entidades federativas y municipales.
Anexo 3: artículo 72, Poderes Legislativos Federal, de las entidades federativas y la Asamblea Legislativa del Distrito Federal.
Anexo 4: artículo 73, Poderes Judiciales Federal y de las entidades federativas.
Anexo 5: artículo 74, fracción I, Instituto Nacional Electoral y organismos públicos locales electorales.
Anexo 6: artículo 74, fracción II, organismos de protección de los derechos humanos Nacional y de las entidades federativas.
Anexo 7: artículo 74, fracción III, organismos garantes del derecho de acceso a la información y la protección de datos personales.
Anexo 8: artículo 75, Instituciones de educación superior públicas dotadas de autonomía.
Anexo 9: artículo 76, partidos políticos nacionales y locales, las agrupaciones políticas nacionales y las personas morales constituidas en asociación civil creadas por los ciudadanos que pretendan postular su candidatura independiente.
Anexo 10: artículo 77, fideicomisos, fondos públicos.
Anexo 11: artículo 78, autoridades administrativas y jurisdiccionales en materia laboral.
Anexo 12: artículo 79, sindicatos que reciban y ejerzan recursos públicos.
Anexo 13: artículo 80, información adicional.
Anexo 14: artículos 81 y 82, personas físicas y morales que reciban y/o ejerzan recursos públicos.
Este instrumento ha tenido varias reformas:

- Publicado Originalmente en el Diario Oficial de la Federación del 04 de mayo de 2016
- Reforma publicada en el Diario Oficial de la Federación del 02 de noviembre de 2016
- Reforma publicada en el Diario Oficial de la Federación del 10 de noviembre de 2016

- Reforma publicada en el Diario Oficial de la Federación del 26 de abril de 2017
- Reforma publicada en el Diario Oficial de la Federación del 28 de diciembre de 2017
- Reforma publicada en el Diario Oficial de la Federación del 28 de diciembre de 2020

A partir de estos anexos se desarrollaron una serie de Tablas de Aplicabilidad que se han ido actualizando de acuerdo con la realidad de cada uno de los sujetos obligados; o de la creación de los mismos.

Fecha DOF	Acta/Dictamen	Nombre
03/11/2016	ACUERDO ACT-PUB/14/09/2016.05	ACUERDO mediante el cual se aprueba la Tabla de aplicabilidad de las obligaciones de transparencia comunes de los sujetos obligados del ámbito federal, en términos del último párrafo del artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública.
13/01/2017	ACUERDO ACT-PUB/07/11/2016.04	ACUERDO mediante el cual se aprueba el procedimiento para la modificación de la tabla de aplicabilidad para el cumplimiento de las obligaciones de transparencia comunes de los sujetos obligados del ámbito federal.
01/09/2017	ACUERDO ACT-PUB/12/07/2017.04	ACUERDO mediante el cual se aprueban las modificaciones al procedimiento para la modificación de la tabla de aplicabilidad para el cumplimiento de las obligaciones de transparencia comunes de los sujetos obligados del ámbito federal.
17/01/2017 [Página INAI]	ACT-PUB/19/04/2017.04	Acuerdo mediante el cual se aprueba el dictamen relativo a la solicitud del Sindicato Nacional de Trabajadores de la Educación, que determina la improcedencia de la modificación a la Tabla de Aplicabilidad de las obligaciones de Transparencia comunes de los sujetos obligados del ámbito Federal.
08/06/2017	ACUERDO ACT-PUB/08/03/2017.04	MODIFICACIÓN a la Tabla de aplicabilidad de las obligaciones de

Fecha DOF	Acta/Dictamen	Nombre
		transparencia comunes de los sujetos obligados del ámbito federal, respecto de las obligaciones de transparencia a cargo del Instituto Nacional Electoral.
03/07/2017	ACUERDO ACT-PUB/07/06/2017.08	MODIFICACIÓN a la Tabla de aplicabilidad de las obligaciones de transparencia comunes de los sujetos obligados del ámbito federal, respecto de las obligaciones de transparencia a cargo de los sindicatos que se indican.
04/12/2017	DICTAMEN DTA 0031/17	MODIFICACIÓN a la Tabla de aplicabilidad de las obligaciones de transparencia comunes de los sujetos obligados del ámbito federal, respecto de las obligaciones de transparencia a cargo de los sindicatos que se indican.
12/07/2018	DICTAMEN DTA 0005/18	MODIFICACIÓN a la Tabla de aplicabilidad de las obligaciones de transparencia comunes de los sujetos obligados del ámbito federal, respecto de las obligaciones de transparencia a cargo del Consejo de la Judicatura Federal.
12/07/2018	DICTAMEN DTA 0006/18	MODIFICACIÓN a la Tabla de aplicabilidad de las obligaciones de transparencia comunes de los sujetos obligados del ámbito federal, respecto de las obligaciones de transparencia a cargo del Partido Encuentro Social.
23/08/2018	DICTAMEN DTA 0011/18	MODIFICACIÓN a la Tabla de aplicabilidad de las obligaciones de transparencia comunes de los sujetos obligados del ámbito federal, respecto de las obligaciones de transparencia a cargo del Sindicato Nacional de Cultura, del Sindicato Nacional de Grupos Artísticos de Bellas Artes y del Sindicato Único de Trabajadores del Instituto Nacional de Bellas Artes y Literatura.
29/08/2019	DICTAMEN DTA 0007/19	MODIFICACIÓN a la tabla de aplicabilidad de las obligaciones de transparencia comunes de los sujetos obligados del ámbito federal, respecto

Fecha DOF	Acta/Dictamen	Nombre
		de las obligaciones de transparencia a cargo de la Secretaría de Seguridad y Protección Ciudadana.
20/02/2020	DICTAMEN DTA 0014/2019	MODIFICACIÓN a la Tabla de aplicabilidad de las obligaciones de transparencia comunes de los sujetos obligados del ámbito federal, respecto de las obligaciones de transparencia a cargo de la Auditoría Superior de la Federación.
16/12/2020	DICTAMEN DTA 0002/20	MODIFICACIÓN a la Tabla de aplicabilidad de las obligaciones de transparencia comunes de los sujetos obligados del ámbito federal, respecto de las obligaciones de transparencia a cargo de la Guardia Nacional, en términos de lo dispuesto en el último párrafo del artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública.
16/12/2020	DICTAMEN DTA 0001/20	MODIFICACIÓN a la Tabla de aplicabilidad de las obligaciones de transparencia comunes de los sujetos obligados del ámbito federal, respecto de las obligaciones de transparencia a cargo de la Agencia Federal de Aviación Civil, en términos de lo dispuesto en el último párrafo del artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública.
16/12/2020	DICTAMEN DTA 0005/20	MODIFICACIÓN a la Tabla de aplicabilidad de las obligaciones de transparencia comunes de los sujetos obligados del ámbito federal, respecto de las obligaciones de transparencia a cargo del Sindicato Patrimonio de Trabajadores y Empleados de la Industria, del Sindicato Nacional de Trabajadores del Instituto Nacional de Bellas Artes y Literatura 227, del Sindicato Democrático Nacional Autónomo de Trabajadores de la Secretaría de Desarrollo Social, del

Fecha DOF	Acta/Dictamen	Nombre
		Sindicato de Investigadores del INIFAP al Servicio del Agro Mexicano, del Sindicato Unificado de Trabajadores del Instituto Nacional de Pediatría y del Sindicato de Trabajadores del Centro de Investigaciones en Óptica, A. C.
20/10/2021	DICTAMEN DTA 0003/21	MODIFICACIÓN a la Tabla de aplicabilidad de las obligaciones de transparencia comunes de los sujetos obligados del ámbito federal, respecto de las obligaciones de transparencia a cargo del Centro Federal de Conciliación y Registro Laboral.
26/11/2021	DICTAMEN DTA 0005/2021	MODIFICACIÓN a la Tabla de aplicabilidad de las obligaciones de transparencia comunes de los sujetos obligados del ámbito federal, respecto de las obligaciones de transparencia a cargo del partido político denominado Fuerza por México, identificado con la clave única 22410, en términos de lo dispuesto en el último párrafo del artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública.
17/12/2021	DICTAMEN DTA 0007/2020	MODIFICACIÓN a la tabla de aplicabilidad de las obligaciones de transparencia comunes de los sujetos obligados del ámbito federal, respecto de las obligaciones de transparencia a cargo del organismo público descentralizado denominado Instituto de Salud para el Bienestar con clave única 12380, en término de lo dispuesto en el último párrafo del artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública.
22/12/2021	DICTAMEN DTA 0008/2021	MODIFICACIÓN a la Tabla de Aplicabilidad de las obligaciones de transparencia comunes de los sujetos obligados del ámbito federal, respecto de las obligaciones de transparencia a cargo del organismo público descentralizado denominado Comisión

Fecha DOF	Acta/Dictamen	Nombre
		Nacional para la Mejora Continua de la Educación, identificado con la clave única 11323, en términos de lo dispuesto en el último párrafo del artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública.

3.6 Tópicos Específicos de la Transparencia y Acceso a la Información Pública

La transparencia es más que solo pedir, recibir y difundir información, es toda una cultura llena de claroscuros; entre los que se debaten por todas las bondades del acceso a la información y los que dicen que, si quieres ocultar algo, se debe poner a la luz de todos.

En este mundo hiperconectado, donde con pocos "clics" nos podemos allegar de todo tipo de información y de datos, públicos y privados, cabe hacernos varias preguntas: ¿Es mejor nuestra sociedad por tener más información? ¿Tener más información nos hace ser mejores? ¿Más información genera más confianza?

Estás preguntas tienen connotaciones que van más allá de lo jurídico; también tienen tintes sociales y por supuestos filosóficos. El filósofo contemporáneo Byung-Chul Hal nos expone varias ideas en su libro intitulado "la sociedad de la transparencia":

- Está demostrado que más información no conduce de manera necesaria a mejoras.[275]
- La sociedad de la transparencia no permite lagunas de información ni de visión.[276]
- La transparencia es un estado de simetría. La sociedad de la transparencia aspira a eliminar todas las relaciones asimétricas. También el poder pertenece a ellas.[277]
- La sociedad de la transparencia es sociedad de la información. En este sentido, la información es, como tal, un fenómeno de la transparencia, porque le falta toda negatividad.[278]
- Un aumento de información y comunicación no esclarece por sí solo el mundo.[279]

[275] Chul Han, Byung, *La sociedad de la transparencia*, España, Herder, 2013, p. 17.
[276] *Ídem*.
[277] *Ibidem*. pp. 39-40.
[278] *Ibidem*. p. 77.
[279] *Ibidem*. p. 79.

- La masa de información no engendra ninguna *verdad*. Cuanta más información se pone en marcha, tanto más intrincado se hace el mundo. La hiperinformación y la hipercomunicación no inyectan ninguna luz en la oscuridad.[280]
- La transparencia y el poder se soportan mal. Al poder le gusta encubrirse en secretos. La praxis arcana es una de las técnicas del poder. La transparencia desmonta la esfera arcana del poder. Pero la transparencia recíproca solo puede lograrse por la vigilancia permanente, que asume una forma siempre excesiva. Esa es la lógica de la sociedad de la vigilancia.[281]
- La sociedad de la transparencia es una sociedad de la desconfianza y de la sospecha, que, a causa de la desaparición de la confianza, se apoya en el control. La potente exigencia de transparencia indica precisamente que el fundamento moral de la sociedad se ha hecho frágil, que los valores morales, como la honradez y la lealtad, pierden cada vez más su significación. En lugar de la resquebrajadiza instancia moral se introduce la transparencia como nuevo imperativo social.[282]

3.6.1. Cultura de transparencia

La Real Academia Española define a la cultura como: […]

> 2. f. Conjunto de conocimientos que permite a alguien desarrollar su juicio crítico.
> 3. f. Conjunto de modos de vida y costumbres, conocimientos y grado de desarrollo artístico, científico, industrial, en una época, grupo social, etc.[283]

Entonces se podría decir que esta cultura de la transparencia es el resultado de como la sociedad y las instituciones han ido evolucionando en la forma de saber pedir y saber entregar la información, rendir cuentas, etc.

Esta cultura de la transparencia ha ido evolucionando a lo largo de los años. El INEGI ha tratado de medir por medio de la Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales (ENAID), la cual recaba información relevante sobre el grado de conocimiento de los derechos de acceso a la información y de protección de datos personales, así como los mecanismos para ejercerlos y garantizarlos.[284]

Este ejercicio inició en 2013 y la última encuesta es de 2019, tal como se aprecia

[280] *Ibidem*. p. 80.
[281] *Ibidem*. p. 91.
[282] *Ibidem*. p. 92.
[283] CULTURA. En: Real Academia Española, *Diccionario de la Real Academia*, 2021, [fecha de consulta: 3 de diciembre de 2022]. Disponible en: *https://dle.rae.es/cultura*
[284] Instituto Nacional de Estadística y Geografía, *Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales (ENAID) 2019*, [en línea] México, INEGI-IFT, 2020, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.inegi.org.mx/programas/enaid/2019/*

en la siguiente ilustración:

Imagen: Diferentes etapas de la encuesta ENAID.
Tomada de: Instituto Nacional de Estadística y Geografía, *Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales 2019 (ENAID)*, [en línea] México, INEGI, 2020, *https://www.inegi.org.mx/contenidos/programas/enaid/2019/doc/enaid_2019_principales_resultados.pdf* p.2.

Dentro de la parte conceptual, la ENAID 2019 abarcó lo siguiente:

Perfil sociodemográfico	Derecho de acceso a la información	Consultas sobre trámites y servicios	Obligaciones de transparencia	Solicitudes de información	Derecho a la Protección de datos personales
- Integrantes del hogar y características sociodemográficas. - Equipamiento del hogar. - Equipos de comunicación para el acceso a la información.	- Tipo de información que consulta la población cotidianamente y medios a través de los cuales se realiza. - Interés de la población en la información que genera el gobierno. - Grado de conocimiento sobre la legislación y la institución encargada de garantizar el Derecho de acceso a la información.	- Experiencias de la población al consultar información para resolver dudas, problemas o realizar quejas sobre servicios públicos, trámites o pagos más utilizados. - Grado de satisfacción con la información obtenida a través de consultas.	- Experiencias de la población al interactuar con los sitios de Internet de instituciones gubernamentales. - Facilidad o dificultad para acceder y navegar en sitios de internet de instituciones gubernamentales. - Satisfacción con la información obtenida.	- Interés de la población en realizar solicitudes de información. - Temas de interés sobre los cuales se solicitaría información. - Experiencias de la población al realizar solicitudes de información: - Procedimientos realizados, - Calidad y satisfacción con la información obtenida, - Medios a través de los cuales se solicitó la información.	- Conocimiento de la población sobre el Derecho de Protección de Datos Personales. - Actitudes sobre la difusión de datos personales y experiencias con el mal uso de los mismos. - Percepción y experiencias en relación con los avisos de privacidad aceptados y/o rechazados por la población al hacer entrega de sus datos personales.

Imagen: Cobertura conceptual de la encuesta ENAID 2019.
Tomada de: Instituto Nacional de Estadística y Geografía, *Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales 2019 (ENAID)*, [en línea] México, INEGI, 2020, *https://www.inegi.org.mx/contenidos/programas/enaid/2019/doc/enaid_2019_principales_resultados.pdf* p.5.

Con respecto a los atributos de la información obtenida en páginas de internet de instituciones y gobierno se obtuvo lo siguiente:

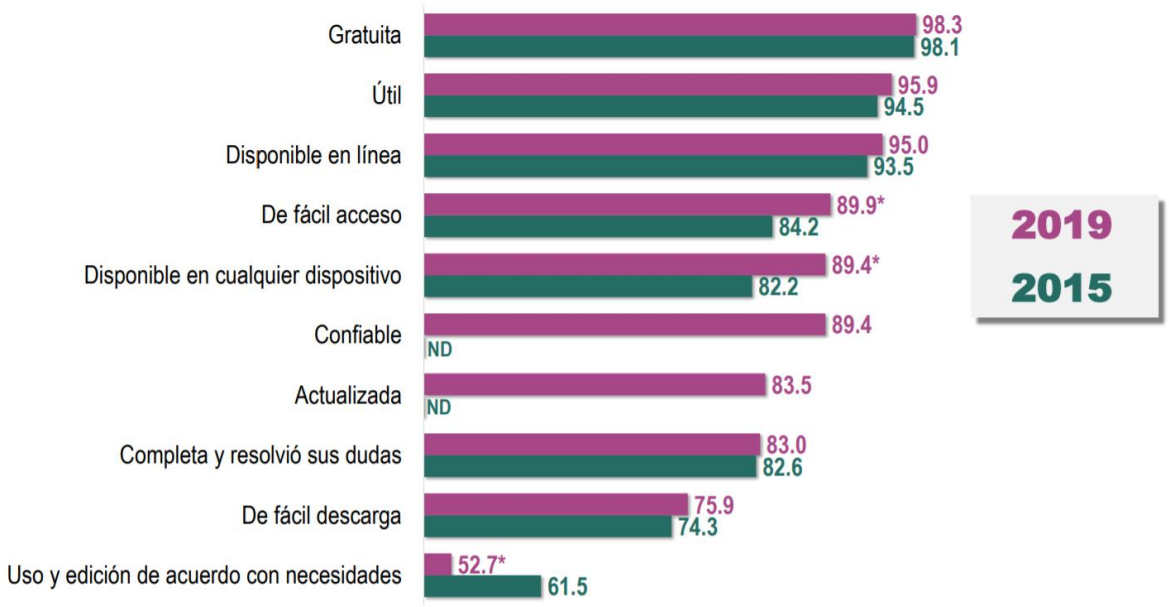


Imagen: Atributos de la información obtenida en páginas de internet de instituciones de gobierno (ENAID 2019).
Tomada de: Instituto Nacional de Estadística y Geografía, *Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales 2019 (ENAID)*, [en línea] México, INEGI, 2020, *https://www.inegi.org.mx/contenidos/programas/enaid/2019/doc/enaid_2019_principales_resultados.pdf* p.47.

Estos avances en materia de transparencia a juicio de Eduardo Guerrero, es que la creación de la cultura de la transparencia y de rendición de cuentas obedece a tres grandes vertientes: "el robustecimiento del control interno o autocontrol de cada uno de los tres poderes federales, la activación del sistema de pesos y contrapesos (los tres poderes empiezan a vigilarse mutuamente), y el avance en la capacidad de la ciudadanía para acceder a la información generada por el gobierno."[285]

Algunas acciones para fomentar la cultura de transparencia han sido las múltiples acciones de capacitación, tanto a sujetos obligados, como a estudiantes, docentes e incluso el público en general. El INAI, el SNT y otros organismos garantes, tienen en sus páginas, multiplicidad de capacitaciones incluyendo la parte en línea de forma gratuita. Otras escuelas como esta Facultad de Derecho promueven la educación en materia de transparencia por medio de diplomados, especialidades, foros y diversos cursos de capacitación a instituciones o en convenio con el propio INAI. Mención sea dicha, un servidor ha participado en varios de estos cursos a sindicatos, sujetos obligados y alumnos que se titulan por medio de Diplomados.

La importancia que tiene la transparencia y el acceso a la información en el manejo de los recursos públicos y su correcta aplicación, busca generar una nueva cultura

[285] Guerrero Gutiérrez, Eduardo, *La luz en busca del cristal hacia la transparencia y la rendición de cuentas en México*, en "Ensayos cultura de transparencia y rendición de cuentas en la gestión pública", [en línea], México, IFE, 2003, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://educacion.michoacan.gob.mx/wp-content/uploads/2015/03/culturatransparenciaddd.pdf* p. 11.

y cambio de actitud en la operación de los programas públicos. En este sentido, fortalecer las acciones para la transparencia, genera mayor confianza lo que se transforma en relaciones comerciales, en atracción de inversiones, nuevos proyectos y en generación de empleo.

Otras acciones están los círculos de lectura, creación de concursos (elaboración de ensayos e investigaciones); foros abiertos, fortalecimiento del gobierno abierto, *data open*, gobernanza en materia de transparencia, acciones con cámaras de comercio, jornadas de derecho a saber, transparencia proactiva, eventos para celebrar el día internacional del Derecho de Acceso a la Información, elaboración de publicaciones especializadas.

El objetivo de todas estas acciones es el de concientizar a las personas sobre su derecho humano de acceso a la información pública, así como para plantear los retos que debemos asumir como sociedad desde nuestros respectivos ámbitos de acción.

Cabe recordar que en algún momento el entonces presidente del INAI Francisco Acuña comentó: "Los mexicanos, somos dados a informarnos. La información, al final de cuentas se requiere, sin importar nuestros orígenes en el interior del país. Los mexicanos somos demasiado confiados y se requiere leer la letra pequeña del instructivo."[286]

Por otra parte, la presidenta del órgano garante en el Estado de México Zulema Martínez Sánchez “subrayó que la cultura de la transparencia debe ser un eje transversal, pues en un plano ideal este, puede ser enseñado desde la educación básica hasta la superior, pues sólo de esa forma se podrán formar ciudadanas y ciudadanos interesados en el funcionamiento de los gobiernos, además de promover e impulsar su ejercicio desde temprana edad.”[287]

3.6.2. Transparencia Pro Activa

La LGTAIP en su título cuarto (Cultura de transparencia y apertura gubernamental), en su capítulo segundo, versa sobre la transparencia proactiva. De ahí que los Organismos garantes emitirán políticas de transparencia proactiva, en atención a los lineamientos generales definidos para ello por el Sistema Nacional, diseñadas

[286] Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco, *Dispersan la cultura de la transparencia, para que la ciudadanía de Yucatán se empodere del Derecho de Acceso a la Información*, [en línea] México, ITEI, 28 de Septiembre de 2020, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.itei.org.mx/v4/prensa/noticias/1524*

[287] Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios, *Necesario promover cultura de la transparencia entre las y los mexiquenses*, [en línea] México, INFOEM, 09 de marzo de 2021, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *http://www.testigossociales.org.mx/es/contenido/noticias/necesario-promover-cultura-de-la-transparencia-entre-las-y-los-mexiquenses*

para incentivar a los sujetos obligados a publicar información adicional a la que establece como mínimo la presente Ley.

Dichas políticas tendrán por objeto, entre otros, promover la reutilización de la información que generan los sujetos obligados, considerando la demanda de la sociedad, identificada con base en las metodologías previamente establecidas.

El pasado 15 de abril de 2016 se publicó el acuerdo del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, por el que se aprueban los Lineamientos para determinar los catálogos y publicación de información de interés público; y para la emisión y evaluación de políticas de transparencia proactiva, mismo que fue modificado el 21 de febrero de 2018 (publicación en el DOF).

Dichos Lineamientos son de observancia obligatoria para los sujetos obligados y tienen por objeto establecer las directrices que deberán observarse para identificar la información adicional que se publicará de manera obligatoria por considerarse de interés público, el procedimiento de remisión al organismo garante para su revisión y el mecanismo de verificación de su cumplimiento, en términos de los artículos 80 y 82 de la Ley General. Así como establecer las reglas y criterios para la emisión de las políticas de transparencia proactiva referidas en los artículos 56, 57 y 58 de la misma Ley, con la finalidad de incentivar a los sujetos obligados a publicar y difundir información adicional a las obligaciones de transparencia comunes y específicas previstas en la Ley General; y establecer los criterios para su evaluación.

Cabe la pena señalar algunas definiciones que vienen en los mismos Lineamientos:

Conocimiento público útil: Aquel valor agregado que ofrece la información procesada o sistematizada, que articula datos, ideas, conceptos y experiencias, a fin de hacerlos del dominio público de manera simple, capaz de permitir el entendimiento y atención de problemas públicos, así como propiciar una toma de decisiones informada, mejorar la calidad de vida de los ciudadanos, fomentar su participación pública y empoderarlos.

Demanda o necesidad de información: Aquella información que la sociedad requiere, sin hacerlo a través de una solicitud de acceso en el marco de las leyes General, Federal o Local en la materia.

Información de calidad: Aquella que publiquen los sujetos obligados y cumpla con los atributos de accesibilidad, confiabilidad, comprensibilidad, oportunidad, veracidad, congruencia, integralidad, actualidad, verificabilidad y que es susceptible de transformarse en conocimiento público útil.

Información de interés público: Aquella que resulta relevante o beneficiosa para la sociedad y no simplemente de interés individual, cuya divulgación resulta útil para que el público comprenda las actividades que llevan a cabo los sujetos obligados.

De acuerdo con los lineamientos expuestos en este apartado, las políticas de transparencia proactiva emitidas por los organismos garantes deberán considerar las siguientes características:

I. Armónica con la normativa vigente: Cumple con las bases, reglas y criterios que establecen las disposiciones en materia de transparencia proactiva;
II. Especializada: El personal de los sujetos obligados será capacitado en materia de transparencia proactiva, con la finalidad de que desarrollen habilidades para la identificación, generación, publicación y difusión de información adicional a la establecida con carácter obligatorio por la Ley General;
III. Progresiva: Procura construir una base inicial de información organizada por categorías, derivado de la identificación de ésta como demanda de la sociedad, y deberá incrementarse gradualmente el volumen y alcance de la información divulgada;
IV. Supervisada: Los organismos garantes supervisarán y evaluarán que los sujetos obligados publiquen información proactiva, de conformidad con los procedimientos que establezca el Instituto para tal efecto, y
V. Validada: Es supervisado, revisado y aprobado en las etapas de identificación, generación, publicación y difusión de información, por el personal responsable, previamente capacitado.

Asimismo, los sujetos obligados podrán establecer procedimientos para la identificación de información a publicar de manera proactiva, debiendo incluir al menos uno de los siguientes:

I. Detección de información que disminuya asimetrías de la información;
II. Detección de información que mejore el acceso a trámites y servicios;
III. Detección de información que optimice la toma de decisiones de autoridades, ciudadanos o población en general, y
IV. Detección de información que detone la rendición de cuentas efectiva.

El objeto de estos procedimientos es la generación de conocimiento público útil enfocado en las necesidades de sectores de la sociedad determinados o determinables, así como aprovechar tanto información generada y/o publicada, como aquella que no ha sido generada, procesada y/o publicada.

Por su parte, y de acuerdo con los lineamientos en comento, los procedimientos para la identificación de información a publicar de manera proactiva, deberán atender al menos las fases siguientes:

I. Detección de información mediante la implementación de mecanismos de participación de la población;
II. Definición del tema, población a la que se dirige, problemática que atiende, demanda o necesidad de información que resuelve;
III. Identificación de contenidos existentes o cuya construcción es necesaria;

IV. Acopio, sistematización y categorización de la información;
V. Generación, publicación y difusión de conocimiento público útil;
VI. Diseño de herramientas e indicadores de medición de reutilización e impacto de la información proactiva, y
VII. Verificación.

De igual forma, la información que se publique en el marco de las políticas de transparencia proactiva deberá ser de calidad, es decir, cumplir los atributos siguientes:

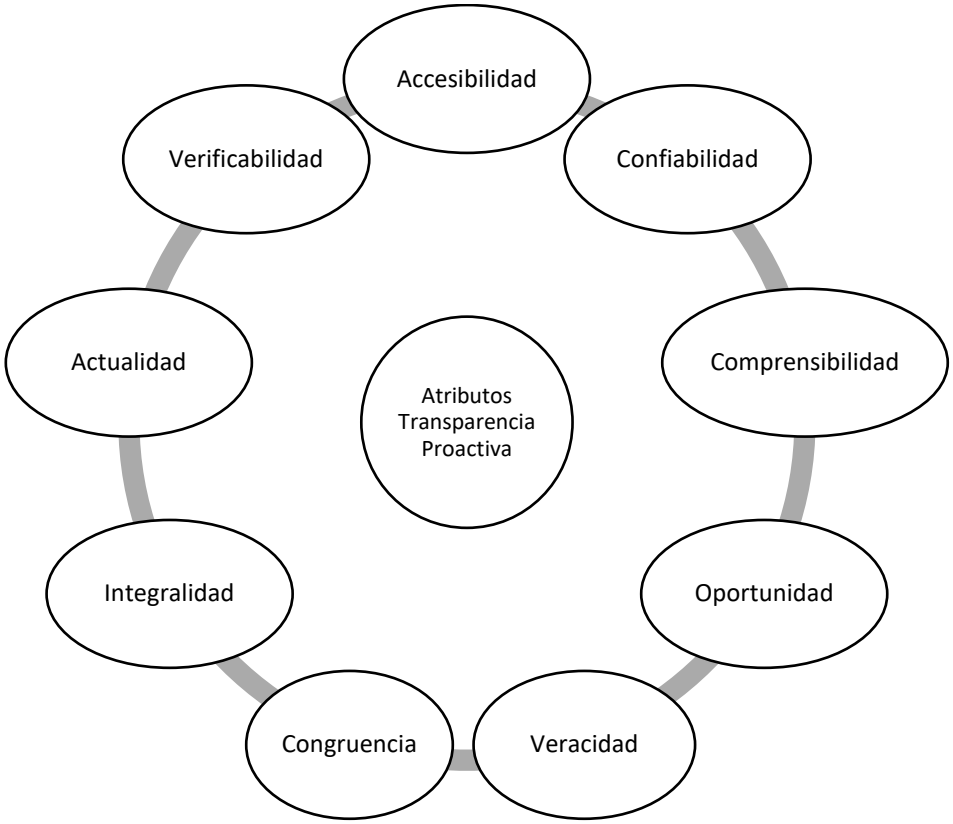


Imagen: Atributos de transparencia proactiva.
Fuente: Elaboración propia. Tomada a partir de los *lineamientos para determinar los catálogos y publicación de información de interés público; y para la emisión y evaluación de políticas de transparencia proactiva*, DOF: 15/04/2016.

El anexo 1 de los Lineamientos indican los procedimientos sugeridos para la identificación de información a publicar de manera proactiva.

I. Procedimiento para la detección de información que disminuya asimetrías de la información.
   a) Método de enfoque directo.
   b) Método de enfoque indirecto.

II. Procedimiento para la detección de información que mejore el acceso a trámites y servicios.

III. Procedimiento para la detección de información que optimice la toma de decisiones de autoridades y ciudadanos.

IV. Procedimiento para la detección de la rendición de cuentas efectiva.

Por otra parte, dentro de los documentos emitidos por el Sistema Nacional de Transparencia se encuentra las Políticas de Gobierno Abierto y Transparencia Proactiva. Estas políticas abonan al cumplimiento de los Objetivos de Desarrollo Sostenible (ODS) particularmente en:

i) Al cumplimiento del ODS 16: "Promover sociedades pacíficas e inclusivas para el desarrollo sostenible, facilitar el acceso a la justicia para todos y *crear instituciones eficaces, responsables e inclusivas a todos los niveles*"
ii) A la articulación de espacios informados de participación ciudadana que permitan la definición, implementación y vigilancia de las políticas públicas orientadas a garantizar el cumplimiento de los 16 ODS restantes.[288]

De la visión y objetivos de la Estrategia 2030 de apertura institucional del INAI se derivan las políticas de transparencia proactiva cuyos rasgos generales son:
Transparencia proactiva: Cualidad inherente a cualquier institución pública que pretende mejorar la comunicación y el diálogo honesto y responsivo con la sociedad; por medio de la identificación, publicación y difusión de información y conocimiento socialmente útil.

Escenarios de la información:

1. La información es asumida como un bien público, y las organizaciones públicas orientan acciones para producir información pertinente y de calidad; es decir, emplean un lenguaje ciudadano y se favorece su publicación en formatos abiertos.
2. La información pública reduce riesgos, mejorar la toma de decisiones, contribuye al ejercicio de los derechos y posibilita procesos efectivos de rendición de cuentas.
3. La información pública está enfocada a la resolución de problemas públicos y es dirigida a audiencias específicas.
4. La información pública reduce espacios de opacidad y prácticas de corrupción, mejora el desempeño y la capacidad de respuesta del gobierno.
5. La información y el conocimiento públicos se difunden y comunican a través de medios considerados adecuados para las audiencias a las que van dirigidos.[289]

Cabe señalar que los organismos garantes también emiten políticas de transparencia proactiva. Por ejemplo, la Comisión de Transparencia y Acceso a la Información del Estado de Nuevo León, el 11 de junio de 2020 emitió el acuerdo mediante el cual se emite la política de transparencia proactiva en atención a los lineamientos generales definidos por el Sistema Nacional de Transparencia, Acceso a la Información pública y protección de datos personales (SNT), a fin de promover

[288] INAI, *Políticas de Gobierno Abierto y Transparencia Proactiva*, [en línea], México, SNT-INAI, s.a., [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://gobiernoabiertogto.org.mx/documentos/libros/46.pdf* p. 9.
[289] *Ibidem*, p. 16.

a los sujetos obligados del Estado a publicar información adicional a la que establece como mínimo la Ley y se deja sin efectos la diversa aprobada en fecha 14 de diciembre de 2017.[290]

3.6.3. Gobierno Abierto

La Ley General de Transparencia en su título cuarto, capítulo tercero, aborda la temática del gobierno abierto indicando en su artículo 59 que los Organismos garantes, en el ámbito de sus atribuciones coadyuvarán, con los sujetos obligados y representantes de la sociedad civil en la implementación de mecanismos de colaboración para la promoción e implementación de políticas y mecanismos de apertura gubernamental.

Por su parte, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) define el gobierno abierto como "una cultura de gobernanza basada en políticas públicas y prácticas innovadoras y sostenibles que se basan a su vez en unos principios de transparencia, rendición de cuentas y participación que promueven la democracia y el crecimiento inclusivo".[291]

El reporte de la OCDE de Gobierno Abierto de 2016, indica que los "países reconocen cada vez más el papel de las reformas de gobierno abierto como catalizadores para la gobernanza pública, la democracia y el crecimiento inclusivo."[292]

De acuerdo con la OCDE, los objetivos de las estrategias de gobierno abierto de los países son las siguientes:

[290] Disponible en Comisión de Transparencia y Acceso a la Información del Estado de Nuevo León, *Acuerdo mediante el cual se emite la política de transparencia proactiva en atención a los lineamientos generales definidos por el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (SNT), a fin de promover a los sujetos obligados del Estado a publicar información adicional a la que establece como mínimo la Ley y se deja sin efectos la diversa aprobada en fecha 14-catorce de diciembre de 2017-dos mil* diecisiete, [en línea] México, COTAI, 2020, [fecha de consulta: 3 de diciembre de 2022] Disponible en: http*://www.cotai.org.mx/descargas/mn/Acuerdo_Politica_Transparencia_Proactiva_18_06_2020.pdf*

[291] Organización para la Cooperación y el Desarrollo Económicos, *Gobierno Abierto, Contexto mundial y el camino a seguir, aspectos claves 2016,* [en línea] EUA, OCDE, 2016, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.oecd.org/gov/Open-Government-Highlights-ESP.pdf* p. 1.

[292] *Ídem*.

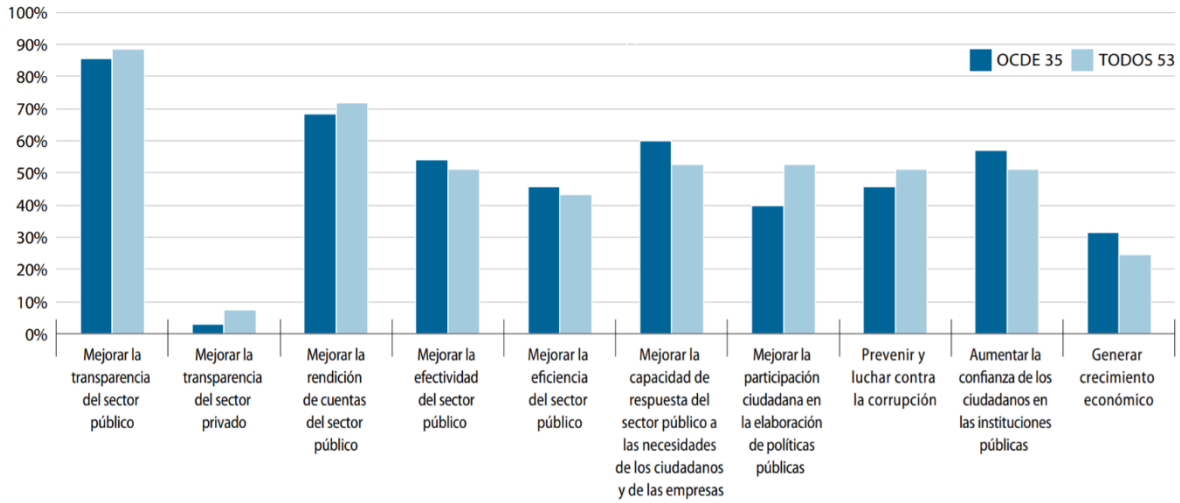


Imagen: Objetivos de las estrategias de gobierno abierto de los países.
Tomada de: Organización para la Cooperación y el Desarrollo Económicos, *Gobierno Abierto, Contexto mundial y el camino a seguir, aspectos claves 2016*, [en línea] EUA, OCDE, 2016, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.oecd.org/gov/Open-Government-Highlights-ESP.pdf* p. 1.

El Marco de trabajo para una estrategia de gobierno abierto según la OCDE es la siguiente:

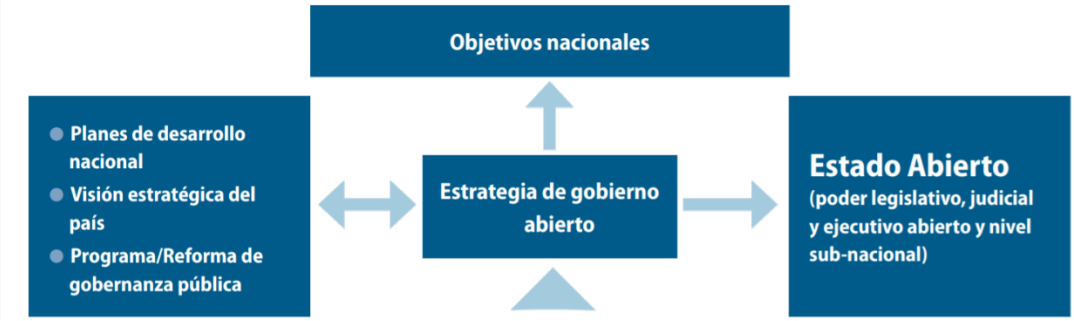


Imagen: Marco de trabajo para una estrategia de gobierno abierto I.
Tomada de: Organización para la Cooperación y el Desarrollo Económicos, *Gobierno Abierto, Contexto mundial y el camino a seguir, aspectos claves 2016*, [en línea] EUA, OCDE, 2016, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.oecd.org/gov/Open-Government-Highlights-ESP*.pdf p. 3.

Imagen: Marco de trabajo para una estrategia de gobierno abierto II.
Tomada de: Organización para la Cooperación y el Desarrollo Económicos, *Gobierno Abierto, Contexto mundial y el camino a seguir, aspectos claves 2016*, [en línea] EUA, OCDE, 2016, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.oecd.org/gov/Open-Government-Highlights-ESP*.pdf p. 3.

La decisión de abordar el gobierno abierto como una nueva forma de hacer buen gobierno se plasmó durante el 66º periodo de sesiones de la Asamblea General de las Naciones Unidas, celebrado en septiembre de 2011, donde se lanzó a nivel mundial el "*Open Government Partnership*"(OGP)[293] Desde su fundación en 2011, OGP ha crecido a 78 países y 76 jurisdicciones locales que trabajan junto a miles de organizaciones de la sociedad civil. Cada dos años, cada miembro presenta un plan de acción creado conjuntamente con la sociedad civil que describe compromisos concretos para mejorar la transparencia, la rendición de cuentas y la participación pública en el gobierno.[294]

La Alianza fue formalmente lanzada en septiembre de 2011, cuando los gobiernos de los ocho países fundadores (Brasil, Indonesia, México, Noruega, Filipinas, Sudáfrica, el Reino Unido y Estados Unidos) adoptaron la Declaración de Gobierno Abierto y anunciaron sus planes de acción. La Alianza fue presentada al mundo en el marco de una conferencia titulada *Open Government Partnership: An International Discussion*, organizada por el Departamento de Estado de Estados Unidos y presidida por la Secretaría de Estado de ese país, Hillary Clinton, así como por el canciller brasileño Antonio Patriota. Por parte de México asistieron representantes del entonces IFAI, la Secretaría de Relaciones Exteriores y el Instituto Mexicano para la Competitividad (IMCO).[295]
La Alianza para el Gobierno Abierto (AGA) es un esfuerzo global para ampliar la frontera en la mejora del desempeño y de la calidad de los gobiernos. Sus fundamentos se encuentran en el hecho de que los ciudadanos desean gobiernos más transparentes, efectivos y que rindan cuentas, con instituciones que robustezcan la participación de la sociedad y respondan a sus necesidades y aspiraciones.[296]

En este sentido los países deben priorizar y escoger al menos uno de estos grandes desafíos en términos de concretar compromisos específicos a través de planes de acción que, además, deberán reflejar y estar guiados por cuatro principios centrales de gobierno abierto propuestos por la AGA: (1) transparencia; (2) participación ciudadana; (3) rendición de cuentas; e (4) innovación y tecnología.[297]

[293] Naser, Alejandra, y Ramírez Alujas, Álvaro, *Plan de Gobierno Abierto, Una hoja de ruta para los Gobiernos de la región*, [en línea], Chile, CEPAL, Serie Manuales, 2017, [fecha de consulta: 3 de diciembre de 2022] Disponible en:
https://repositorio.cepal.org/bitstream/handle/11362/36665/4/S1700687_es.pdf p. 12.
[294] Open Government Partnership, *Miembros*, [en línea], s/d, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.opengovpartnership.org/es/our-members/*
[295] INAI, *¿Qué es la alianza para el Gobierno Abierto?*, [en línea], México, INAI, s.a., [fecha de consulta: 3 de diciembre de 2022] Disponible en:
https://micrositios.inai.org.mx/gobiernoabierto/?page_id=803
[296] Naser, Alejandra, *op. cit*. p.16.
[297] *Ibidem.* p. 19.

Hay autores como Valenzuela Mendoza y Bojórquez, que mencionan que el Gobierno abierto tiene componentes externos e internos como se aprecia en el siguiente cuadro:[298]

Componentes	Dentro de la organización pública (variables endógenas)	Hacia afuera de la organización pública (variables exógenas)
Transparencia Colaborativa	Producir datos abiertos e información pública, en plataforma interoperable	Garantizar al ciudadano el acceso a la información pública
Participación colaborativa	Crear mecanismos de tratamiento de ideas y procesar la innovación. Inteligencia gubernamental abierta a ciudadanos.	Fomentar la inclusión de la ciudadanía, vía organizaciones no gubernamentales, especializadas en temas. Inteligencia colectiva abierta al gobierno.
Creación de valor social	Modelos de gestionar lo público en forma transparente e interactiva. Una administración más deliberativa	Intervención digital y política de la ciudadanía en procesos de política y gestión públicas

México, por su parte, reconoce como pilares del Gobierno abierto:[299]

1) Transparencia y Acceso a la información.
2) Rendición de Cuentas.
3) Participación.
4) Colaboración.

En el caso de la tecnología, se ve más de una manera transversal que apoya en el cumplimiento de los pilares del Gobierno Abierto. Ahora bien, esta parte electrónica da lugar a la pregunta si es lo mismo el gobierno abierto que el gobierno electrónico, para lo cual puede servir el siguiente cuadro:[300]

Gobierno Electrónico	Gobierno Abierto
1) Utiliza la tecnología para mejorar cualitativamente los servicios e	1) Involucra a la ciudanía en la toma de decisiones.

[298] Valenzuela Mendoza, Rafael Enrique y Bojórquez Pereznieto, José Antonio, *Modelos de implementación del Gobierno Abierto en México*, en "Gobierno Abierto y el Valor de la información pública", [en línea] México, UNAM-IIJ, 2016, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://archivos.juridicas.unam.mx/www/bjv/libros/9/4016/9.pdf* p. 134.
[299] INAI, *El ABC del Gobierno Abierto,* [en línea], México, INAI, 2020, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/digital_el_abc.pdf* pp. 10-11.
[300] Basado el *Ibidem*. pp. 12-14.

2) información que se ofrece a los ciudadanos. 3) Se enfoca a la voluntad y la capacidad del gobierno para utilizar la tecnología para llevar a cabo sus funciones con mayor eficiencia y constituye una herramienta para facilitar la provisión de bienes públicos para un mayor número de personas. 4) Algunos casos del gobierno electrónico son la gestión de trámites y servicios por medios remotos, sin requerir que los ciudadanos acudan físicamente a las oficinas del gobierno.	2) Trabajar de la mano con la sociedad utilizando 3) diversos medios y tecnologías para generar más y mejores políticas públicas que atiendan las necesidades de la sociedad. 4) Se construye a partir de un ciclo de diálogo constante con los ciudadanos para conocer sus necesidades y así tomar decisiones conjuntas, lo que permite maximizar los beneficios sociales.

Para avanzar en la agenda de gobierno abierto, en México fue constituido el Secretariado Técnico Tripartita o STT (compuesto por representantes de las organizaciones de la sociedad civil, un representante de Presidencia de la República y un representante del INAI), a continuación, se presentan algunas de las acciones realizadas por este órgano:[301]

- Visión de México para la Presidencia de la Alianza para el Gobierno Abierto 2014-2015
- Diagnóstico de cumplimiento Plan de Acción Ampliado 2011-2012
- Decálogo de puntos relevantes a considerar en la Ley General de Transparencia
- Balance de AGA en México
- Libro de Resultados del Plan de Acción México 2013-2015
- Derechos humanos y fortalecimiento del Estado de Derecho
- Igualdad de Género
- Pobreza y Desigualdad
- Servicios Públicos de Salud
- Sistema Nacional Anticorrupción
- Servicios Públicos de Agua
- Gobernanza y Recursos Naturales

En México, el documento más reciente en materia de Gobierno Abierto el ámbito Federal es el 4° Plan de Acción 2019-2021 de México de los cuales surgieron los siguientes compromisos:[302]

[301] INAI, *¿Qué es la alianza para el Gobierno Abierto?*, INAI, *op. cit.*

[302] Alianza para el Gobierno Abierto México, *4° Plan de Acción 2019-2021 de México*, [en línea] México, SFP-INAI, 2019, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.opengovpartnership.org/wp-content/uploads/2019/12/Mexico_Action-Plan_2019-2021.pdf* p. 8.

Compromisos Cocreados	Compromisos Proactivos
1. Gasto abierto y responsable en programas sociales	7. Controles democráticos a la intervención de comunicaciones privadas
2. Incidencia ciudadana para el desarrollo rural sustentable	8. Fortalecer los servicios públicos de cuidados
3. Información transparente y de calidad para garantizar el derecho a la educación	9. Transparencia para el monitoreo y vigilancia de los fideicomisos
4. Derechos sexuales y reproductivos para las y los jóvenes	10. Fortalecimiento de la transparencia sobre la gestión de bosques, agua y pesca
5. Transparencia para fomentar la inclusión laboral	11. Hacia la divulgación de beneficiarios finales
6. Plataforma única y abierta de información de seguridad pública	12. Transparencia del flujo y control de armas
	13. Estrategia subnacional de gobierno abierto

Imagen: Temáticas por tipo de compromiso.
Tomada de: Alianza para el Gobierno Abierto México, *4° Plan de Acción 2019-2021 de México*, [en línea] México, SFP-INAI, 2019, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.opengovpartnership.org/wp-content/uploads/2019/12/Mexico_Action-Plan_2019-2021.pdf* p. 8.

El gobierno abierto también abarca acciones locales; las entidades federativas, también tienen planes de gobierno abierto, para lo cual sirve el siguiente cuadro:[303]

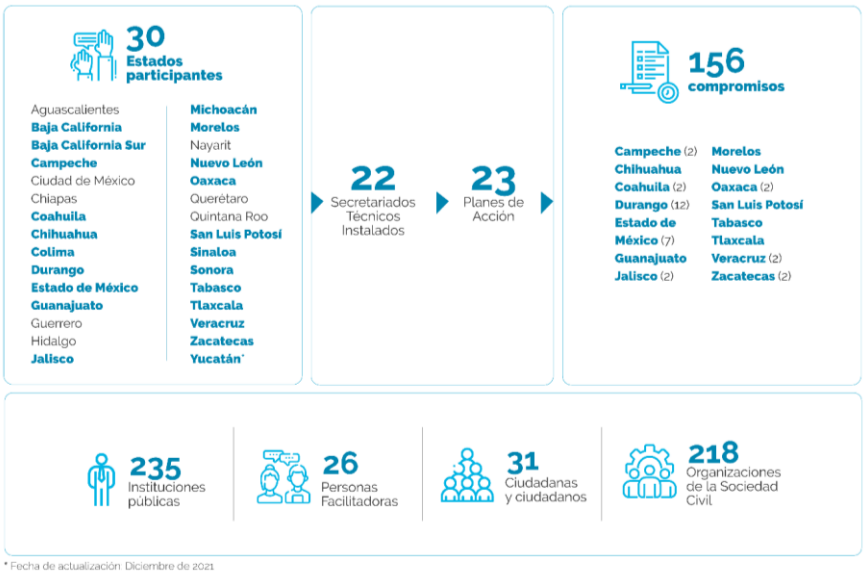


Imagen: Estrategia de cocreación desde lo local Entidades Federativas.
Tomada de: INAI, *Cocreación desde lo local*, [en línea], México, INAI, s.a. [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://micrositios.inai.org.mx/gobiernoabierto/?page_id=877*

Solamente Tamaulipas y Puebla no participan en esta iniciativa. A continuación, se presenta como se han ido sumando las entidades federativas desde 2015, así como

[303] INAI, *Cocreación desde lo local*, [en línea], México, INAI, s.a. [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://micrositios.inai.org.mx/gobiernoabierto/?page_id=877*

los pasos para implementar una estrategia local de Gobierno Abierto.[304]
De acuerdo con el INAI, los pasos para que una entidad federativa implemente una estrategia local de Gobierno Abierto son los siguientes:

Imagen: Pasos para implementar una estrategia local de Gobierno Abierto.
Tomada de: INAI, *Cocreación desde lo local*, [en línea], México, INAI, s.a. [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://micrositios.inai.org.mx/gobiernoabierto/?page_id=877*

3.6.3.1. Datos Abiertos

En 2015, se desarrolló y presentó la Carta Internacional de Datos Abiertos. Dicha carta fue desarrollada “por gobiernos, la sociedad civil y expertos de todo el mundo como un conjunto de normas acordadas a nivel mundial sobre cómo publicar datos.”[305]

De acuerdo con esta carta, los datos abiertos “son datos digitales que son puestos a disposición con las características técnicas y jurídicas necesarias para que puedan ser usados, reutilizados y redistribuidos libremente por cualquier persona, en cualquier momento y en cualquier lugar.”

En el preámbulo de esta carta se reconocen como beneficios de los datos abiertos los siguientes:

1) Permite a los actores públicos, privados y sociales tomar mejores decisiones informadas.
2) Permiten comparar, combinar y seguir las conexiones entre distintos conjuntos de datos.

[304] *Ídem*.
[305] *Open Data Charter, Carta Internacional de Datos Abiertos, Resumen*, [en línea] ODC, s.a., [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://opendatacharter.net/principles-es/*

3) Pueden empoderar a los actores públicos, privados y sociales para trabajar hacia mejores resultados para servicios públicos.
4) Pueden contribuir a la generación de crecimiento económico inclusivo al apoyar la creación y el fortalecimiento de nuevos mercados, empresas y empleos.
5) Coadyuvan a mejorar el fujo de información en el sector público, mejorando los procesos de transparencia, rendición de cuentas, buena gobernanza y combate a la corrupción.
6) Brindan soluciones con políticas públicas innovadoras y basadas en evidencia, y fomentar beneficios económicos y desarrollo social para todos los integrantes de la sociedad.[306]

La carta reconoce como principios los siguientes:[307]

1) Abiertos por Defecto
2) Oportunos y Exhaustivos;
3) Accesibles y Utilizables
4) Comparables e Interoperables
5) Para mejorar la Gobernanza y la Participación Ciudadana
6) Para el Desarrollo Incluyente y la Innovación

El 28 de octubre de 2015, México se adhirió a la Carta Internacional de Datos Abiertos, comprometiéndose a trabajar mediante la Política de Datos Abiertos para implementar sus Principios.[308]

La interrelación de los datos abiertos, *big data* y gobierno abierto ha dado lugar a seis subtipos diferentes de datos con rasgos comunes procedentes de cada una de las categorías madre, tal y como se muestra en el gráfico anterior, pero que, dependiendo de la intersección de éstas, presentan características diferentes:[309]

- **Grandes datos, pero no abiertos.** Datos de compra, información clínica, registros de transacciones económicas… Gran cantidad de macrodatos se engloba dentro de esta categoría, la mayoría con un importante valor comercial. Su tratamiento y reutilización es de gran utilidad tanto para el sector público como privado ya que, gracias a ellos, se puede predecir patrones comerciales, tendencias demográficas o brotes epidemiológicos.
- **Gobierno abierto, sin apertura de datos.** El movimiento open government aboga por la participación ciudadana en las decisiones de los gobiernos

[306] Basado en *Open Data Charter*, *Carta Internacional de Datos Abiertos*, [en línea] ODC, 2015, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://transparencia.gob.gt/wp-content/uploads/Carta_Internacional_de_Datos_Abiertos2015.pdf* pp. 1-4.
[307] *Ídem*.
[308] Secretaría de la Función Pública, *Política de Transparencia, Gobierno Abierto y Datos Abiertos de la Administración Pública Federal 2021-2024*, [en línea] México, SFP, 2021, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://funcionpublica.gob.mx/web/transparencia/Politica_de_Transparencia_Gobierno_Abierto_y_Datos_Abiertos_de_la_APF_2021-2024.pdf* p. 30.
[309] Gobierno de España, *Datos abiertos, big data y gobierno abierto: diferentes tipos de datos,* [en línea] España, Portal "datos.gob.es"2017, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://datos.gob.es/es/noticia/datos-abiertos-big-data-y-gobierno-abierto-diferentes-tipos-de-datos*

locales, regionales o nacionales. Sin embargo, esta corriente no siempre incluye políticas de datos abiertos y, en ocasiones, no conlleva la apertura de la información del sector público.

- **Big data, abiertos pero no gubernamentales.** Actualmente, existe una gran cantidad de datos que no proceden de organismos públicos, sino de fuentes académicas, empresariales o privadas, con un enfoque abierto y reutilizable. La publicación de los resultados de investigaciones científicas como en el caso del buscador Zooniverse o la reutilización del *social data*, como Wenalyze, son solo algunos ejemplos de datos masivos y abiertos, pero no públicos.
- **Datos gubernamentales, pero no big data.** Los datos del gobierno no tienen por qué ser masivos para ser valiosos. La publicación de una cantidad modesta de información pública, como por ejemplo los horarios de transporte público, puede tener un impacto positivo en la sociedad gracias al desarrollo de nuevos productos o servicios de valor añadido.
- **Datos abiertos y privados.** Esta categoría incluye aquellos datos del sector privado que las empresas deciden abrir para sus propios fines, por ejemplo, para satisfacer a posibles inversores o mejorar su reputación corporativa. Los *hackathones* que organizan las entidades financieras a partir de su propia información es una buena muestra de esta categoría de datos abiertos.
- **Datos abiertos, *big data* y gobierno abierto.** El trinomio perfecto. La apertura de estos conjuntos de datos puede tener un gran impacto socioeconómico en su entorno. De hecho, según estadísticas del portal europeo de datos, la reutilización de los datos abiertos podría salvar 7.000 vidas al año o ahorrar hasta 629 mil millones de horas en las carreteras.

Lo anterior se puede ver condensado en la siguiente ilustración:[310]

[310] *Ídem*.

Imagen: Elementos del Gobierno Abierto.
Tomada de: Gobierno de España, *Datos abiertos, big data y gobierno abierto: diferentes tipos de datos,* [en línea] España, Portal "datos.gob.es"2017, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://datos.gob.es/es/noticia/datos-abiertos-big-data-y-gobierno-abierto-diferentes-tipos-de-datos*

Cabe destacar que no es lo mismos Datos Abiertos que Gobierno Abierto, para lo cual sirve el siguiente cuadro:[311]

Datos Abiertos	Gobierno Abierto
Se habla EXCLUSIVAMENTE de datos con mayor potencial de uso, cuyas características de apertura se refieren a la publicación de datos con: **Licencias o Términos de Libre Uso**, que hagan explícita la posibilidad de usar los datos para cualquier cosa (e.g. Términos de Libre Uso MX, *Open Government License UK, Creative Commons Attribution* 4.0), y **Formatos de archivo no propietarios**, cuyas especificaciones técnicas están disponibles públicamente, que no supongan dificultad de acceso, y que su aplicación y reproducción o estén condicionadas a contraprestación alguna (e.g. .CSV, .JSON).	Cuando hablamos de gobierno, la característica de apertura se refiere a un esquema de gobernanza que siguen los principios de la Declaración de la Alianza para el Gobierno Abierto: 1) Aumentar la disponibilidad de información sobre las actividades gubernamentales, 2) Apoyar la participación ciudadana, 3) Aplicar los más altos estándares de integridad profesional en todos nuestros gobiernos, y 4) Aumentar el acceso a las nuevas tecnologías para la apertura y la rendición de cuentas.

Por su parte, la Ley General de Transparencia en su artículo 3° fracción VI. Dispone lo siguiente:

> Datos abiertos: Los datos digitales de carácter público que son accesibles en línea que pueden ser usados, reutilizados y redistribuidos por cualquier interesado y que tienen las siguientes características:
>
> a) Accesibles: Los datos están disponibles para la gama más amplia de usuarios, para cualquier propósito;
>
> b) Integrales: Contienen el tema que describen a detalle y con los metadatos necesarios;
>
> c) Gratuitos: Se obtienen sin entregar a cambio contraprestación alguna;
>
> d) No discriminatorios: Los datos están disponibles para cualquier persona, sin necesidad de registro;

[311]Zapata, Enrique, *La diferencia entre Datos Abiertos y Gobierno Abierto*, [en línea], México, Datos Abiertos México, 17 de abril de 2018, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://datos.gob.mx/blog/la-diferencia-entre-datos-abiertos-y-gobierno-abierto*

e) Oportunos: Son actualizados, periódicamente, conforme se generen;

f) Permanentes: Se conservan en el tiempo, para lo cual, las versiones históricas relevantes para uso público se mantendrán disponibles con identificadores adecuados al efecto;

g) Primarios: Provienen de la fuente de origen con el máximo nivel de desagregación posible;

h) Legibles por máquinas: Deberán estar estructurados, total o parcialmente, para ser procesados e interpretados por equipos electrónicos de manera automática;

i) En formatos abiertos: Los datos estarán disponibles con el conjunto de características técnicas y de presentación que corresponden a la estructura lógica usada para almacenar datos en un archivo digital, cuyas especificaciones técnicas están disponibles públicamente, que no suponen una dificultad de acceso y que su aplicación y reproducción no estén condicionadas a contraprestación alguna;

j) De libre uso: Citan la fuente de origen como único requerimiento para ser utilizados libremente;

A su vez, el artículo 51 de la misma Ley General dispone que los Organismos garantes promoverán la publicación de la información de Datos Abiertos y Accesibles.

Con base en la Ley General, actualmente el pasado 30 de junio de 2021, se publicó el acuerdo por el que se emite la Política de Transparencia, Gobierno Abierto y Datos Abiertos de la Administración Pública Federal 2021-2024.

Dicha política, es un conjunto de disposiciones administrativas que permitirán a la Secretaría de la Función Pública conducir las acciones del gobierno federal en materia de transparencia, gobierno abierto y datos abiertos de manera holística, integral, diferencial e interdependiente, para contribuir a la rendición de cuentas y al combate de la corrupción e impunidad.

La Política de Transparencia, Gobierno Abierto y Datos Abiertos de la Administración Pública Federal 2021-2024, es de observancia obligatoria para las dependencias y entidades de la Administración Pública Federal, las cuales deberán considerar los ejes estratégicos, prioridades y acciones de la misma.

La Unidad de Transparencia y Políticas Anticorrupción de la Secretaría de la Función Pública, dará seguimiento a la implementación de los ejes estratégicos, prioridades y acciones establecidos en la Política de Transparencia, Gobierno Abierto y Datos Abiertos de la Administración Pública Federal 2021-2024; así como realizar las evaluaciones correspondientes.

Asimismo, cada sujeto obligado y Organismo Constitucional tienen planes de Datos Abiertos y páginas *ex profeso* de Datos Abiertos.

3.6.3.2. Gobierno Abierto desde el punto de vista de la Sociedad Civil

La sociedad civil tuvo una nueva forma de participar en la política pública a partir de 2004 con la publicación de la Ley Federal de Fomento a las Actividades Realizadas por Organizaciones de la Sociedad Civil. Las OSC participarían de manera más activa en cuestiones de Gobernanza.

En el ejercicio ciudadano del derecho de acceso a la información, se han constituido diversas organizaciones civiles que promueven la transparencia, así como el derecho de acceso a la información, siendo una de ellas el denominado Colectivo por la Transparencia el cual a 2018 está integrado por otras OSC como:[312]

Alianza Cívica	Información Accesible y Rendición de Cuentas (IARAC)
Visión Legislativa	Centro Mexicano de Derecho Ambiental
Colectivo Ciudadanos por Municipios Transparentes (CIMTRA)	Cultura Ecológica
DECA- Equipo Pueblo	Fundar, Centro de Análisis e Investigación
GESEC Gestión social y cooperación	ONG Contraloría Ciudadana para la rendición de cuentas
Sonora Ciudadana	Iniciativa Sinaloa
Centro Nacional de Comunicación Social (CENCOS)	Equis Justicia para las Mujeres
Gente Diversa de Baja California	Alternativas y Capacidades

Actualmente, el núcleo de organizaciones de la sociedad civil de la alianza de gobierno abierto en México es un espacio de colaboración de doce asociaciones civiles sin fines de lucro, comprometidas con establecer una estrategia común ante los Planes de Acción de Gobierno Abierto en México, así como para tener un grupo cohesionado con un mensaje compartido ante esta agenda. Las asociaciones civiles que conforman este grupo son: Artículo 19 Oficina para México y Centroamérica; Causa Natura, A.C.; Contraloría Ciudadana para la Rendición de Cuentas; Cultura Ecológica; Equis Justicia para las Mujeres, A.C.; Fundar, Centro de Análisis e Investigación; GESOC, Agencia para el Desarrollo A.C.; Instituto de Liderazgo Simone de Beauvoir; Instituto Mexicano para la Competitividad, A.C.; México Evalúa; Observatorio Nacional Ciudadano; SocialTIC y Transparencia Mexicana.

[312] Morales Tostado, María del Carmen, *Participación de la sociedad civil en el derecho de acceso a la información pública*, en BIOLEX, Revista Jurídica del Departamento de Derecho de la Universidad de Sonora, [en línea] México, Vol. 12, No. 22, enero-junio 2020, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://biolex.unison.mx/index.php/biolex_unison_mx/issue/view/23/31* pp. 96-97.

Indica Fernando Gutiérrez que los “nuevos medios digitales de comunicación se han convertido en un indispensable instrumento de expresión política de la sociedad civil y eventualmente, en una importante herramienta de presión nacional e internacional para la transparencia y el acceso a la información pública”.[313]

Las OSC como se pudo apreciar se asocian, partición y fomentan en diferentes foros, concursos, coadyuvancia con las autoridades en todos los diferentes órdenes de gobierno. “Desde la información a la co-decisión, puede observarse un nivel creciente de participación y de influencia ciudadana en la elaboración de políticas públicas, y la influencia que ejercen los ciudadanos en la elaboración de dichas políticas públicas se incrementa.”[314] A continuación, se presenta la escalera imaginaria de las prácticas participativas de la OCDE:

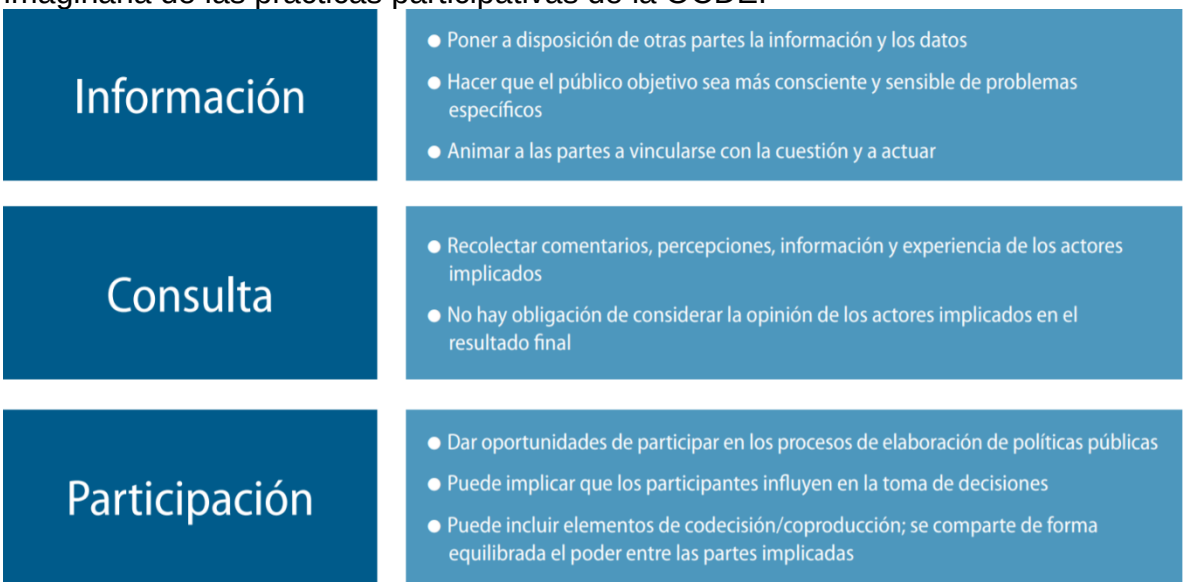


Imagen: Escalera imaginaria de las prácticas participativas: Niveles de participación de los actores implicados.
Tomada de: Organización para la Cooperación y el Desarrollo Económicos, *Gobierno Abierto, Contexto mundial y el camino a seguir, aspectos claves 2016*, [en línea] EUA, OCDE, 2016, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *https://www.oecd.org/gov/Open-Government-Highlights-ESP.pdf* p. 12.

El propósito de la participación ciudadana abarca un amplio espectro de posibilidades que van desde la información hasta el control de la actividad gubernamental. Tal como se aprecia en el siguiente cuadro:[315]

---

[313] Gutiérrez, Fernando, *Los nuevos medios digitales como herramienta de la sociedad civil para la transparencia y el acceso a la información pública*, en “Panel: Sociedad Civil y Transparencia”, [en línea] México, ITAIPEM, Memoria Tercera Semana Estatal de Transparencia, mayo de 2008, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *http://contraloriadelpoderlegislativo.gob.mx/Revista_Rc_et_Ratio/Rc_et_Ratio_1/Rc1_2_Sociedad_civil_y_transparencia.pdf* p. 28.
[314] OCDE, *Gobierno Abierto, op. cit*. p. 12.
[315] Navarro, Erick, *De los mecanismos de participación ciudadana a la consolidación de gobierno abierto*, en Naser Alejandra (Coord), “Gobierno abierto y ciudadanía en el centro de la gestión pública”, [en línea], CEPAL, ONU, 2021, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://repositorio.cepal.org/bitstream/handle/11362/47256/1/S2100371_es.pdf* p. 95.

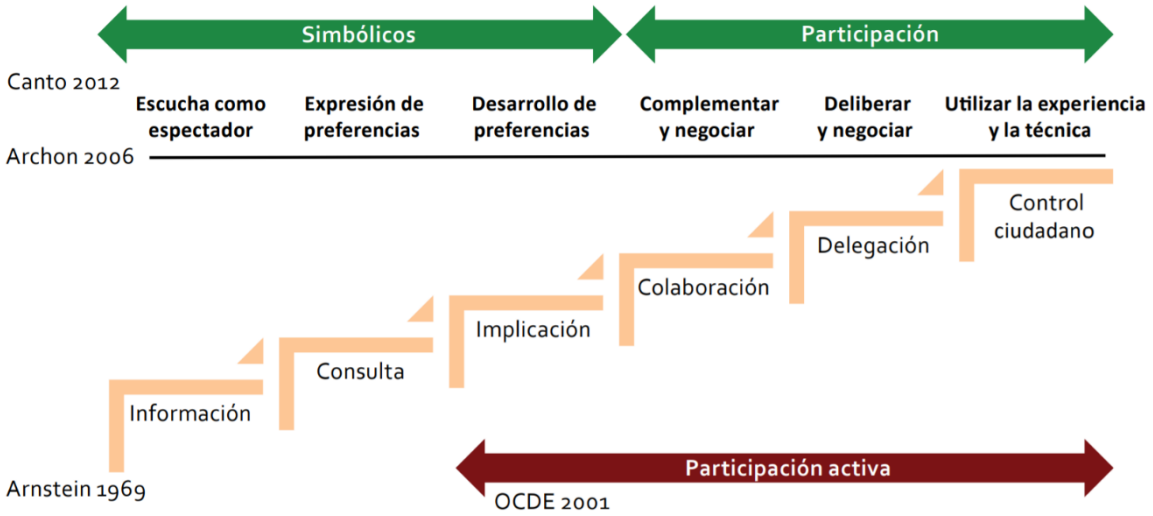


Imagen: Propósito de la participación ciudadana.
Tomada de: Navarro, Erick, *De los mecanismos de participación ciudadana a la consolidación de gobierno abierto*, en Naser Alejandra (Coord), "Gobierno abierto y ciudadanía en el centro de la gestión pública", [en línea], CEPAL, ONU, 2021, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://repositorio.cepal.org/bitstream/handle/11362/47256/1/S2100371_es.pdf* p. 95.

Por su parte, dentro de las funciones y responsabilidades que tienen la sociedad civil, son:

- Monitorear: Responsables del monitoreo al desempeño de sus autoridades.
- Verificar: Elemento clave para detonar y acompañar procesos de rendición de cuentas.
- Levantar la voz y abandonar las negociaciones: Derecho a hacer valer su voz.
- Identificar: Contribuir a la identificación de necesidades y problemas públicos prioritarios.
- Guiar al gobierno en los compromisos: Cocrear compromisos de la mano de sus autoridades para la atención de problemas públicos.
- Representar de manera plural: Ser representado de manera plural en el ejercicio.
- Dar seguimiento a los compromisos: Dar seguimiento a la implementación de los compromisos adquiridos por autoridades y ciudadanos.
- Evitar conflictos de interés: Evitar conflictos de interés durante su participación en cualquier ejercicio de apertura.
- Privilegiar acciones colectivas: Privilegiar acciones colectivas sobre los proyectos individuales.[316]

Finalmente, dentro de los incentivos para que las OSC continúen involucrándose están los siguientes:[317]

[316] INAI, *Gobierno Abierto y Transparencia Proactiva. Manual del Participante*, [en línea] México, INAI, 2017, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://transparencia.info.jalisco.gob.mx/sites/default/files/manualgaimprenta.pdf* p. 59.
[317] *Ibidem*. pp. 60-61.

1) Incidencia: Capacidad de las organizaciones para introducir cambios y mejoras en las estrategias y programas de gobierno.
    a. Ubicarse en discusiones centrales de política pública en una determinada entidad federativa.
    b. Establecer contacto con “líderes” dentro del gobierno, interesados en impulsar cambios en las estrategias políticas.
    c. Identificar “puntos de encuentro” con el gobierno que permitirá ampliar los márgenes de incidencia.
2) Respaldo: Posibilidad de encontrar eco de agendas de las organizaciones de la sociedad civil como parte de su participación en esquemas de cocreación.
    a. Participar en espacios y discusiones con autoridades y funcionarios que pueden apoyar los diagnósticos y propuestas.
    b. Contar potencialmente con el respaldo político de alto nivel para impulsar la agenda.
    c. Establecer “equipos” con otras organizaciones involucradas e intercambiar ideas, conocimiento y experiencia, y avanzar agendas conjuntas.
    d. Amplificar mensajes entre otras audiencias a través de las plataformas de cocreación.
3) Visibilidad y recursos: Estrategias de gobierno abierto como herramientas que pueden ampliar la presencia y el acceso a financiamiento por parte de organizaciones de la sociedad civil.
    a. Fortalecer la presencia en debates públicos a nivel estatal, ampliando las audiencias que visibilizan las propuestas.
    b. Acceso a redes de financiamientos (nacionales e internacionales) que privilegian proyectos construidos en colaboración.
4) Visibilidad y recursos: Estrategias de gobierno abierto como herramientas que pueden ampliar la presencia y el acceso a financiamiento por parte de organizaciones de la sociedad civil.
    a. Fortalecer la presencia en debates públicos a nivel estatal, ampliando las audiencias que visibilizan las propuestas.
    b. Acceso a redes de financiamientos (nacionales e internacionales) que privilegian proyectos construidos en colaboración.
    c. Vinculación con otras plataformas de diálogo y cocreación, impulsadas a escala nacional y en otras entidades federativas, potenciando los márgenes de incidencia.

3.6.4. Manejo de la información Clasificada

El derecho de acceso a la información puede ser limitado, de manera excepcional, cuando:[318]

[318] Secretaría de la Función Pública, *Guía para ejercer el derecho de Acceso a la información Pública*, [en línea], México, SFP, s.a., [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://www.gob.mx/cms/uploads/attachment/file/428425/DDP_Gu_a_Informacion_Publica_13Dic1*

I. Existan razones de interés público.
II. Se trate de información de seguridad nacional.
III. Se trate de información confidencial.

Cuando alguno de los tres supuestos señalados se actualiza, los sujetos obligados pueden clasificar la información que se encuentra en su posesión, como reservada o confidencial, según sea el caso, tal como se aprecia en el siguiente cuadro:[319]

RESERVADA	CONFIDENCIAL
Se trata de aquella información que aun cuando es pública no puede difundirse, ya que generaría un daño, por lo que es necesario acreditar, la afectación que se causaría de ser revelada.	Es aquella información que contiene datos personales. También los secretos bancario, fiduciario, industrial, comercial, fiscal, bursátil y postal de particulares, sujetos de derecho internacional o a sujetos obligados, cuando no involucren el ejercicio de recursos públicos.
Temporal y excepcional.	No está sujeta a un plazo.
Se justifica por razones de interés público o seguridad nacional previstas en la Ley General.	Se justifica porque se trata de datos personales o secretos cuya titularidad es de particulares, y no involucran recursos públicos.
Requiere de la aplicación de la prueba de daño.	Requiere describir con base en la normatividad que se trata de datos personales o un secreto.

En los casos en los que la información se clasifique parcialmente, es decir, cuando solo una sección, párrafo o palabra es la que no puede entregarse por ser clasificada, el sujeto obligado otorgará acceso a la información que sí es pública, manteniendo clasificada aquella información que no debe publicarse.

De esta manera, cuando los documentos o expedientes contengan información pública y clasificada, se podrá generar una versión pública.

Una versión pública es “el documento a partir del que se otorga acceso a la información, en el que se testan partes o secciones clasificadas, indicando el contenido de éstas de manera genérica, fundando y motivando la reserva o confidencialidad, a través de la resolución que para tal efecto emita el Comité de Transparencia.”[320]

8.pdf p. 14.
[319] *Ídem*.
[320] Sistema Nacional de Transparencia, *Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas*, [en línea] Diario Oficial de la Federación del 15 de abril de 2016, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://www.dof.gob.mx/nota_detalle.php?codigo=5433280&fecha=15/04/2016#gsc.tab=0*

Cabe señalar que el pasado 15 de abril de 2016 se publicó en el Diario Oficial el Acuerdo del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, por el que se aprueban los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

La carga de la prueba para justificar toda negativa de acceso a la información, por actualizarse cualquiera de los supuestos de clasificación previstos en la Ley General, la Ley Federal y leyes estatales, corresponderá a los sujetos obligados, por lo que deberán fundar y motivar debidamente la clasificación de la información ante una solicitud de acceso o al momento en que generen versiones públicas para dar cumplimiento a las obligaciones de transparencia, observando lo dispuesto en la Ley General y las demás disposiciones aplicables en la materia.

Los sujetos obligados no podrán emitir acuerdos de carácter general ni particular que clasifiquen documentos o expedientes como reservados, ni clasificar documentos antes de que se genere la información o cuando éstos no obren en sus archivos.

La clasificación de información se realizará conforme a un análisis caso por caso, mediante la aplicación de la prueba de daño y de interés público.

Sobre este tema, el Pleno de la Corte ha sostenido que la clasificación de la información como reservada corresponde al desarrollo del límite previsto en el artículo 6o. constitucional referente a la protección del interés público, mientras que la categoría de información confidencial responde a la necesidad de proteger la vida privada de las personas y sus datos personales. Desde esta perspectiva, resulta necesario entender que la relación entre el derecho a la información y sus límites, en cuanto se fundamentan en otros bienes constitucionalmente tutelados, no se da en términos absolutos de todo o nada, sino que su interacción es de carácter ponderativo, en la medida en que la natural tensión que pueda existir entre ellos, requiere en su aplicación un equilibrio necesario entre el ejercicio efectivo del derecho a la información y la indebida afectación de otro tipo de bienes y valores constitucionales que están instituidos también en beneficio de las personas. Es por ello que, si se reconoce que ningún derecho humano tiene el carácter de absoluto, entonces debe igualmente reconocerse que ninguno de sus límites puede plantearse en dichos términos, por lo que la relación entre ambos extremos debe plantearse en los mismos términos de equilibrio.[321]

Asimismo, de acuerdo con el artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, y con los lineamientos segundo, fracción XIII y trigésimo tercero, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones

[321] DERECHO A LA INFORMACIÓN. LA RELACIÓN CON SUS LÍMITES CONSTITUCIONALES NO DEBE PLANTEARSE EN TÉRMINOS ABSOLUTOS. Tesis: P. II/2019 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. I, enero de 2020, p. 561.

públicas, aprobados por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales y publicados en el Diario Oficial de la Federación el 15 de abril de 2016, la prueba de daño es la argumentación fundada y motivada que deben realizar los sujetos obligados para acreditar que la divulgación de la información lesiona un interés jurídicamente protegido y que el daño que puede producir es mayor que el interés de conocer ésta. Para tal efecto, disponen que en la clasificación de la información pública (como reservada o confidencial), debe justificarse que su divulgación representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional; que ese riesgo supera el interés público general de que se difunda; y, que la limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio. Así, la prueba de daño establece líneas argumentativas mínimas que deben cursarse, a fin de constatar que la publicidad de la información solicitada no ocasionaría un daño a un interés jurídicamente protegido, ya sea de índole estatal o particular. Por tanto, al tratarse de un aspecto constreñido al ámbito argumentativo, la validez de la prueba de daño no depende de los medios de prueba que el sujeto obligado aporte, sino de la solidez del juicio de ponderación que se efectúe en los términos señalados.[322]

Cabe señalar que México forma parte de los “Principios de Lima”[323] de 16 de noviembre de 2000, el cual en su numeral 8, señala las excepciones al acceso a la información: “Las leyes de privacidad no deben inhibir ni restringir la investigación y difusión de información de interés público. La ley, habiendo determinado los casos específicos de información clasificada, establecerá plazos y procedimientos razonables para su desclasificación tan pronto como el interés de seguridad nacional lo permita.”[324]

Para clasificar la información como reservada, debe hacerse un análisis, caso por caso, mediante la aplicación de la "prueba de daño". Sin perjuicio de lo anterior, cuando un documento contenga partes o secciones reservadas o confidenciales, los sujetos obligados deberán elaborar una versión pública, en la que testen única y exclusivamente aquéllas, con indicación de su contenido de forma genérica, así como la fundamentación y motivación que sustente dicha clasificación. Por otra parte, si alguien intenta revertir determinada clasificación de información que estima no es confidencial, debe plantearlo ante la autoridad que realizó la clasificación, dando audiencia a los beneficiados con la decretada y a los probables afectados,

---

[322] PRUEBA DE DAÑO EN LA CLASIFICACIÓN DE LA INFORMACIÓN PÚBLICA. SU VALIDEZ NO DEPENDE DE LOS MEDIOS DE PRUEBA QUE EL SUJETO OBLIGADO APORTE. Tesis: I.10o.A.79 A (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. III, noviembre de 2018, p. 2318.

[323] Los principios tienen como fundamento que el acceso a la información es un derecho fundamental en una sociedad democrática y debe ser asegurado por el Estado a todos los ciudadanos sin distinción.

[324] Organización de Estados Americanos, *Principios de Lima*, [en línea] OEA, s.a., [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=158&lID=2*

para el evento de que se reclasifique, a través de la "prueba del interés público". De lo anterior se advierte que corresponde a los sujetos obligados realizar la clasificación de la información que obre en su poder y, contra la decisión que adopten, procede interponer el recurso de revisión ante el organismo garante que corresponda. En consecuencia, la obligación de clasificar la información corresponde única y directamente a los sujetos obligados, en tanto que al Juez de amparo sólo compete facilitar, bajo su más estricta responsabilidad, el acceso a la que sea "indispensable para la adecuada defensa de las partes".[325]

Por último, la diferencia entre la prueba de daño y la prueba de interés público, es la siguiente:

PRUEBA DE DAÑO	PRUEBA DE INTERÉS PÚBLICO
Realizada por Sujetos Obligados	Realizada por Órganos Garantes
Es para clasificar la información	Es para controvertir la clasificación de la información
Describir los elementos del riesgo que conlleva la difusión de la información al bien tutelado (real/presente; demostrable/probable e identificable/específico.	Proceso de ponderación entre el beneficio que reporta dar a conocer la información pedida o solicitada contra el daño que su divulgación genera en los derechos de las personas.
El valor jurídicamente protegido es el interés colectivo del Estado, traducido en un bien público.	El valor protegido es la vida privada o el patrimonio de las personas.
Cuando los valores en conflicto determinan que, en el mismo ejemplo, la publicidad pone en riesgo a la seguridad, se concluye con la reserva del documento.[326]	Cuando los valores en conflicto determinan que debe prevalecer el interés público sobre la vida privada, se procede a la divulgación.

De forma particular cabe señalar la figura llamada **inexistencia de información**. Sobre el particular, la Ley General indica en su artículo 19 que se presume que la información debe existir si se refiere a las facultades, competencias y funciones que los ordenamientos jurídicos aplicables otorgan a los sujetos obligados. En los casos en que ciertas facultades, competencias o funciones no se hayan ejercido, se debe motivar la respuesta en función de las causas que motiven la inexistencia.

[325] ACCESO A LA INFORMACIÓN. EJERCICIO DEL DERECHO RELATIVO TRATÁNDOSE DE LA CLASIFICADA COMO CONFIDENCIAL, MEDIANTE LA PRUEBA DE DAÑO O DEL INTERÉS PÚBLICO Y ROL DEL JUEZ DE AMPARO PARA FACILITAR LA DEFENSA DE LAS PARTES. Tesis: I.1o.A.E.133 A (10a.), Semanario Judicial de la Federación, Décima Época, t. III, abril de 2016, p. 2133.

[326] Robertos (*sic)* Chuc, Juan Carlos, *Clasificación de la Información y Archivos Públicos*, en Instituto de Acceso a la Información y Protección de Datos Personales de Quintana Roo, “8° Certamen de Ensayo en Materia de Transparencia y Acceso a la información Pública”, México, IDAIPQROO, 2016, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *http://www.idaipqroo.org.mx/wp-content/uploads/2017/07/octavo_ensayo.pdf* p. 16.

De lo anterior se desprende que la inexistencia implica necesariamente que la información no se encuentra en los archivos de la autoridad -es decir, se trata de una cuestión de hecho-, no obstante que la dependencia o entidad cuente con facultades para poseer dicha información. En este sentido, es de señalarse que la inexistencia es un concepto que se atribuye a la información solicitada.

El propósito de que los Comités de Transparencia emitan una declaración que confirme la inexistencia de la información solicitada, es garantizar al solicitante que se realizaron las gestiones necesarias para la ubicación de la información de su interés; por lo cual, el acta en el que se haga constar esa declaración formal de inexistencia, debe contener los elementos suficientes para generar en los solicitantes la certeza del carácter exhaustivo de la búsqueda de lo solicitado. [327]

3.7. Procedimientos en materia de Transparencia

Con la nueva ley de transparencia, se pueden diferenciar diferentes procedimientos que se podrían separar en ordinarios y medios de defensa siendo los siguientes:

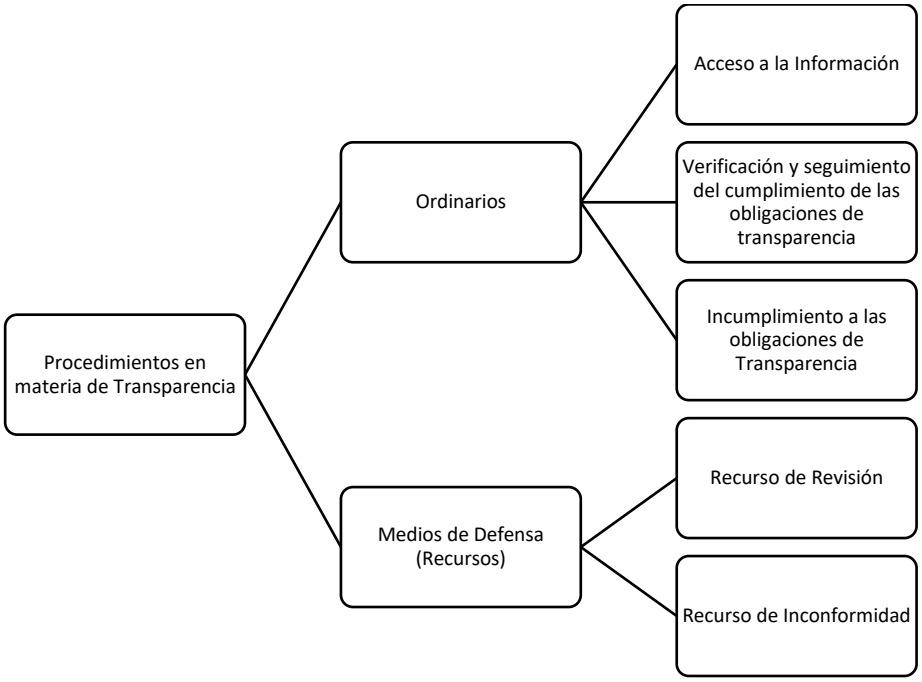


Imagen: Procedimientos en materia de transparencia.
Fuente: Elaboración propia.

El procedimiento de acceso a la información está regulado en el capítulo primero del título séptimo de la Ley General, así como en el acuerdo mediante el cual se aprueban los lineamientos que establecen los procedimientos internos de atención

[327] INAI, *Propósito de la declaración formal de inexistencia*, [en línea] México, INAI, 2019, ACUERDO ACT-PUB/11/09/2019.06. Segunda época, criterio 04/19. [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://stprmnacional.org/transparencia/Criterios/19/Criterio04-19.pdf*

a solicitudes de acceso a la información pública, publicados en el Diario Oficial el 12 de febrero de 2016.

Los lineamientos tienen por objeto establecer las reglas para la recepción, procesamiento, trámite de las solicitudes de acceso a la información, que formulen los particulares, así como en su resolución, notificación y la entrega de la información, con excepción de las solicitudes en materia de protección de datos personales.

Los lineamientos son de observancia obligatoria para los sujetos obligados que son: cualquier autoridad, entidad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal.

Los formatos aprobados por el Sistema Nacional de Transparencia para la presentación de las solicitudes de acceso a la información, estarán disponibles tanto impresos como en medios electrónicos en las unidades de transparencia, en la oficina o las oficinas designadas para ello, representaciones y delegaciones que cuenten con personal habilitado, así como en la Plataforma Nacional.
El procedimiento de Acceso a la Información se puede resumir en la siguiente imagen:[328]

[328] Alternativas y Capacidades, A.C., *Mecanismos de acceso a la información para la reconstrucción*, [en línea] México, s.a., [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://alternativasycapacidades.org/noticias/mecanismos-acceso-informacion/*

Imagen: Procedimiento de Acceso a la Información.
Tomada de: Alternativas y Capacidades, A.C., *Mecanismos de acceso a la información para la reconstrucción*, [en línea] México, s.a., [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://alternativasycapacidades.org/noticias/mecanismos-acceso-informacion/*

Cada unidad de transparencia de los sujetos obligados, cuenta con su manual de procedimientos en materia de transparencia, donde se esquematizan las acciones al interior dl sujeto obligado.

Cabe señalar que actualmente disponemos de diferentes herramientas tecnológicas para acceder a la información, las cuales están enlazadas a la plataforma nacional de transparencia, tal como se aprecia en el siguiente cuadro:

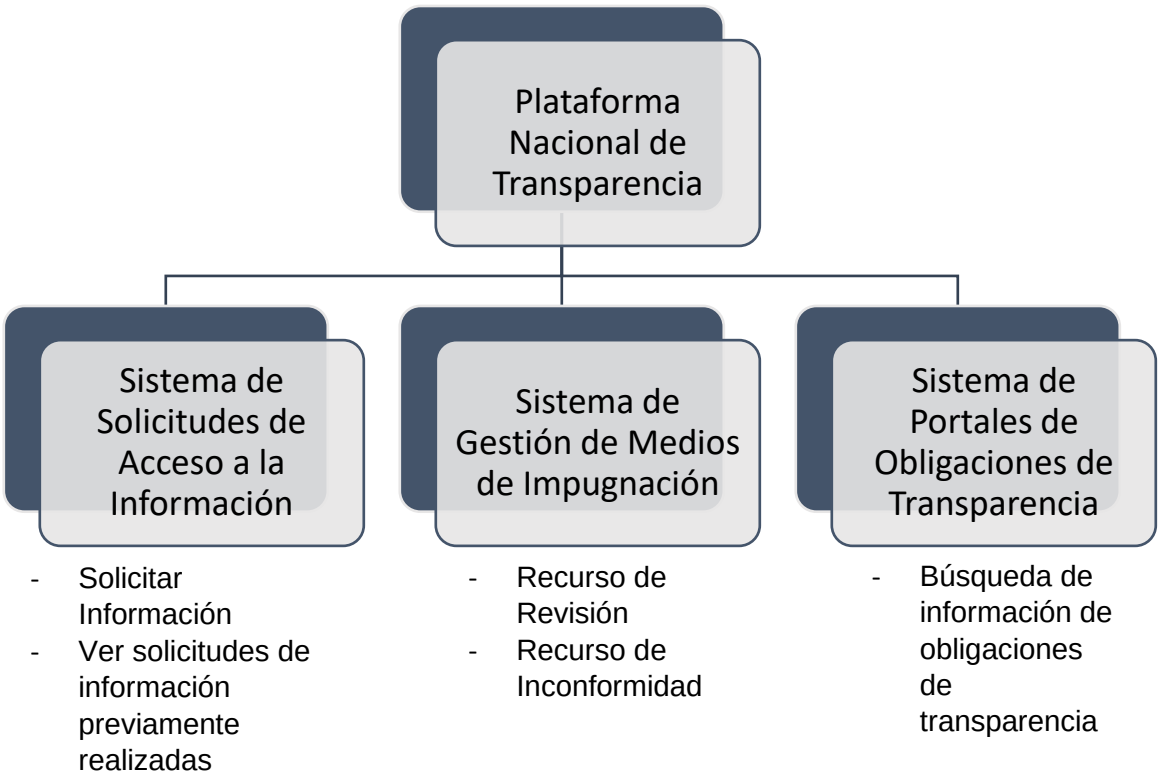


Imagen: Plataforma Nacional de Transparencia.
Fuente: Elaboración propia.

Otro procedimiento ordinario es el de verificación y seguimiento del cumplimiento de las obligaciones de transparencia, el cual tiene como fundamento los artículos 70 a 83 de la Ley General, así como los Lineamientos que establecen el procedimiento de verificación y seguimiento del cumplimiento de las obligaciones de transparencia (DOF: 20/02/2017); así como el acuerdo mediante el cual se modifican los lineamientos que establecen el procedimiento de verificación y seguimiento del cumplimiento de las obligaciones de transparencia que deben publicar los sujetos obligados del ámbito federal en los portales de internet y en la Plataforma Nacional de Transparencia; así como el manual de procedimientos y metodología de evaluación para verificar el cumplimiento de las obligaciones de transparencia que deben de publicar los sujetos obligados del ámbito federal en los portales de internet y en la Plataforma Nacional de Transparencia, (DOF: 30/04/2018).

Los Lineamientos son de observancia general y obligatoria para el Instituto y los sujetos obligados del ámbito federal, y tienen como propósito regular el procedimiento de verificación al cumplimiento de las obligaciones de transparencia previstas en los artículos 70 a 83 de la Ley General de Transparencia y Acceso a la Información Pública y 68 a 76 de la Ley Federal de Transparencia y Acceso a la Información Pública.

Las acciones de vigilancia se realizarán mediante la verificación de los portales de internet y de la Plataforma Nacional, a efecto de corroborar que la información publicada por los sujetos obligados esté completa y que la actualización haya sido realizada en tiempo y forma, es decir, que cuente con los elementos de forma, términos, plazos y formatos establecidos en los Lineamientos Técnicos Generales y en los Lineamientos Técnicos Federales.

De acuerdo con el Manual, estos procedimientos de verificación pueden ser de oficio (censal o muestral), o apetición de parte.

Asimismo, el Manual establece la metodología de evaluación para la verificación del cumplimiento de las obligaciones de transparencia, el cual tienen como propósito comprobar que la información publicada por los sujetos obligados en sus portales de internet y en la Plataforma Nacional, cuente con los elementos mínimos de contenido, confiabilidad, actualización y formato previstos en los lineamientos de publicación en portales.

Otro procedimiento ordinario es el de incumplimiento a las obligaciones de transparencia el cual tiene como fundamento el artículo 90 de la Ley General, así como los lineamientos que establecen el procedimiento de denuncia por incumplimiento a las obligaciones de transparencia previstas en los artículos 70 a 83 de la Ley General de Transparencia y Acceso a la Información Pública y 69 a 76 de la Ley Federal de Transparencia y Acceso a la Información Pública, (DOF: 17/02/2017); así como el acuerdo mediante el cual se modifican los lineamientos que establecen el procedimiento de denuncia por incumplimiento a las obligaciones de transparencia previstas en los artículos 70 a 83 de la Ley General de Transparencia y Acceso a la Información Pública y 69 a 76 de la Ley Federal de Transparencia y Acceso a la Información Pública, (DOF: 30/04/2018).

Los lineamientos son de observancia obligatoria para el Instituto y los sujetos obligados en el ámbito federal, y tienen como propósito regular el procedimiento de denuncia por incumplimiento a las Obligaciones de Transparencia previstas en los artículos 70 a 83 de la Ley General de Transparencia y Acceso a la Información Pública y 69 a 76 de la Ley Federal de Transparencia y Acceso a la Información Pública, así como la falta de actualización de las mismas.

El procedimiento de la denuncia se integra por las siguientes etapas:

I. Presentación de la denuncia ante el Instituto;
II. Solicitud por parte del Instituto al sujeto obligado de un informe justificado respecto de los hechos o motivos de la denuncia;
III. Resolución de la denuncia, y
IV. Ejecución de la resolución de la denuncia.

Pasamos ahora a los medios de defensa que puede interponer el particular, y donde

podemos señalar el recurso de revisión, y el recurso de inconformidad.

El recurso de revisión, tiene su fundamento en el capítulo I del título octavo de la Ley General, relativo al “recurso de revisión ante los organismos garantes”, artículos 142 a 158. Este recurso es el medio legal con el que cuentan los particulares para impugnar la respuesta de los sujetos obligados a sus solicitudes de acceso a la información pública.

Procede el recurso de revisión cuando en la respuesta:

- Se clasifique información.
- Se declare la inexistencia de la información.
- Se declare la incompetencia.
- Se entregue información incompleta.
- No corresponda la información con lo solicitado.
- No se dé respuesta a la solicitud.
- La modalidad o formato sea distinta a la solicitada.
- Se entregue la información en un formato incomprensible y/o no accesible para el solicitante.
- Cuando exista inconformidad con los costos o tiempos de entrega de la información.
- No se le dé trámite a una solicitud.
- Exista negativa a permitir la consulta directa de la información.
- Exista falta, deficiencia o insuficiencia de la fundamentación y/o motivación en la respuesta,
- Se oriente a un trámite específico.

Se puede presentar el recurso de revisión ante el INAI, o ante el organismo garante que corresponda en cada entidad federativa, o bien, ante la Unidad de Transparencia que haya conocido de la solicitud. Se tiene un plazo de 15 días siguientes a la fecha de la notificación de respuesta, o del vencimiento del plazo para su notificación.

El Pleno del INAI es la autoridad encargada de resolver los recursos de revisión en contra de las respuestas proporcionadas por los sujetos obligados del ámbito federal. Los Sujetos Obligados de las entidades federativas cuentan con sus propios organismos garantes encargados de conocer y resolver las controversias en materia de acceso a la información. Se pueden consultar en la siguiente página de Internet: http://www.plataformadetransparencia.org.mx/

El INAI tiene un plazo máximo de 40 días a partir de que se admita el recurso de revisión. Este plazo puede ampliarse por una sola vez y hasta por 20 días más.

Por su parte, el recurso de inconformidad, tiene su fundamento en el capítulo II del título octavo de la Ley General, relativo al recurso de inconformidad, artículos 159 a 180. El recurso de inconformidad es un procedimiento con el que cuenta el titular para manifestar su desacuerdo sobre las resoluciones emitidas por los organismos

garantes estatales. El INAI se pronuncia sobre las mismas como una segunda instancia.

El recurso de inconformidad debe presentarse ante el Instituto dentro de un plazo de quince días hábiles a partir del siguiente a la fecha de la notificación de la resolución impugnada. Si el titular interpone el recurso de inconformidad ante los organismos garantes estatales, debe remitir el recurso 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 recurso de inconformidad procederá contra las resoluciones emitidas por los organismos de las entidades federativas que:

I. Confirmen o modifiquen la clasificación de la información, o
II. Confirmen la inexistencia o negativa de información.
Se entenderá como negativa de acceso a la información la falta de resolución de los Organismos garantes de las Entidades Federativas dentro del plazo previsto para ello.

El Instituto resolverá el recurso de inconformidad en un plazo que no podrá exceder de treinta días, plazo que podrá ampliarse por una sola vez y hasta por un periodo igual.

Interpuesto el recurso de inconformidad por falta de resolución, en términos del segundo párrafo del artículo 160 de esta Ley, el Instituto dará vista, en el término de tres días siguientes, contados a partir del día en que fue recibido el recurso, al organismo garante de la Entidad Federativa según se trate, para que alegue lo que a su derecho convenga en un plazo de cinco días.

Recibida la contestación, el Instituto deberá emitir su resolución en un plazo no mayor a quince días. En caso de no recibir la contestación por parte del organismo garante de la entidad federativa, o que éste no pruebe fehacientemente que dictó resolución o no exponga de manera fundada y motivada, a criterio del Instituto, que se trata de información reservada o confidencial, el Instituto resolverá a favor del solicitante.

La resolución del Instituto será definitiva e inatacable para el organismo garante y el sujeto obligado de que se trate.
Los particulares podrán impugnar las resoluciones del Instituto ante el Poder Judicial de la Federación.

Capítulo 4. Régimen Jurídico de la Protección de Datos Personales

De la innumerable cantidad y tipos de datos que existen, los datos personales, revisten una particular forma de protección, dada la trascendencia que tiene el cuidado, e implicaciones con otros derechos como la intimidad, la privacidad y los

propios datos personales.

El párrafo segundo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos reconoce los denominados derechos ARCO, relativos al acceso, rectificación, cancelación y oposición de datos personales, como un medio para garantizar el derecho de los individuos a decidir qué aspectos de su vida deben o no ser conocidos o reservados por el resto de la sociedad, y la posibilidad de exigir su cumplimiento a las autoridades y particulares que conocen, usan o difunden dicha información. Así, dichas prerrogativas constituyen el derecho a la protección de los datos personales, como un medio de salvaguarda de otros derechos fundamentales previstos en la propia Constitución y en los tratados internacionales de los que México es parte, conforme a los cuales, el Estado tiene la obligación de garantizar y proteger el derecho de todo individuo a no ser interferido o molestado por terceros o por una autoridad, en ningún aspecto de su persona –vida privada–, entre los que se encuentra el relativo a la forma en que se ve a sí mismo y cómo se proyecta a los demás –honor–, así como de aquellos que corresponden a los extremos más personales de la vida y del entorno familiar –intimidad–, o que permiten el desarrollo integral de su personalidad como ser humano –dignidad humana–.[329]

En este sentido, los textos constitucionales y los tratados internacionales de derechos humanos recogen el derecho a la intimidad como una manifestación concreta de la separación entre el ámbito privado y el público. Así, el derecho a la intimidad se asocia con la existencia de un ámbito privado que se encuentra reservado frente a la acción y conocimiento de los demás y tiene por objeto garantizar al individuo un ámbito reservado de su vida frente a la acción y conocimiento de terceros, ya sea simples particulares o bien los Poderes del Estado; tal derecho atribuye a su titular el poder de resguardar ese ámbito reservado por el individuo para sí y su familia; asimismo garantiza el derecho a poseer la intimidad a efecto de disponer del control sobre la publicidad de la información tanto de la persona como de su familia; lo que se traduce en el derecho de la autodeterminación de la información que supone la posibilidad de elegir qué información de la esfera privada de la persona puede ser conocida o cuál debe permanecer en secreto, así como designar quién y bajo qué condiciones puede utilizar esa información. En este contexto, el derecho a la intimidad impone a los poderes públicos, como a los particulares, diversas obligaciones, a saber: no difundir información de carácter personal entre los que se encuentran los datos personales, confidenciales, el secreto bancario e industrial y en general en no entrometerse en la vida privada de las personas; asimismo, el Estado a través de sus órganos debe adoptar todas las medidas tendentes a hacer efectiva la protección de este derecho.[330]

[329] PROTECCIÓN DE DATOS PERSONALES. CONSTITUYE UN DERECHO VINCULADO CON LA SALVAGUARDA DE OTROS DERECHOS FUNDAMENTALES INHERENTES AL SER HUMANO. Tesis: I.10o.A.5 CS (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. III, septiembre de 2019, p. 2199.

[330] DERECHO A LA INTIMIDAD. SU OBJETO Y RELACIÓN CON EL DERECHO DE LA AUTODETERMINACIÓN DE LA INFORMACIÓN. Tesis: I.3o.C.695 C., Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XXVIII, septiembre de 2008, p. 1253.

Ahora bien, ¿Qué tratamiento o protección deben de ser sujetos los datos de las personas morales? Las normas y algunas interpretaciones de los tribunales federales no se ponen totalmente de acuerdo en si las personas morales tienen o no datos "personales" y por ende pudiesen llegar a ser titulares de protección de datos personales como con las personas físicas.

Las leyes de protección de datos personales tanto la General como la Federal en Posesión de Particulares, refieren en sus definiciones de Datos personales, solamente a Personas Físicas de la siguiente manera:

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO)	Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP)
Artículo 3. Para los efectos de la presente Ley se entenderá por: 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;	Artículo 3.- Para los efectos de esta Ley, se entenderá por: V. Datos personales: Cualquier información concerniente a una **persona física** identificada o identificable.

Por su parte, el Reglamento de la Ley Federal del Protección de Datos Personales en Posesión de Particulares dispone:

> Artículo 5. Las disposiciones del presente Reglamento no serán aplicables a la información siguiente:
> I. La relativa a personas morales; […]

La guía para cumplir con los principios y deberes de la LFPDPPP indica que: "La información relativa a una persona moral no se considera como dato personal, quedando ésta excluida de la protección que otorga la normatividad sobre protección de datos personales a las personas físicas."[331]

En el caso del Poder Judicial, la segunda sala de la Suprema Corte de Justicia de la Nación (SCJN) llegó a considerar que "al tutelar sólo el derecho a la protección de datos personales de las personas físicas y no de las morales, colectivas o jurídicas privadas, no violan la indicada garantía contenida en el artículo 1o. de la Constitución Política de los Estados Unidos Mexicanos, pues tal distinción se justifica porque el derecho a la protección de los datos personales se refiere

[331] INAI, *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, [en línea] México, INAI, 2016, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Guia_obligaciones_lfpdppp_junio2016.pdf* p. 3.

únicamente a las personas físicas por estar encausado al respeto de un derecho personalísimo, como es el de la intimidad, del cual derivó aquél. Esto es, en el apuntado supuesto no se actualiza una igualdad jurídica entre las personas físicas y las morales porque ambas están en situaciones de derecho dispares, ya que la protección de datos personales, entre ellos el del patrimonio y su confidencialidad, es una derivación del derecho a la intimidad, del cual únicamente goza el individuo, entendido como la persona humana."[332]

Adicionalmente, y ya en plena décima época, se emitió una tesis "sobre la base de que toda persona física es titular de derechos humanos, se deriva que el reconocimiento de éstos es una consecuencia de la afirmación de la dignidad humana, por lo que no puede actualizarse violación a aquéllos respecto de una persona moral, pues ésta constituye un ente ficticio y, por ende, carente del factor relativo a la dignidad humana, […] de manera que, partiendo de un análisis básico, al contextualizar las dos unidades semánticas que componen la expresión "derechos humanos", la primera palabra está utilizada como la facultad que le asiste a una persona y, la segunda, alude a que la única propiedad que ha de satisfacerse para ser titular de estos derechos es la de pertenecer a los seres humanos, lo que significa que excluye a las personas morales."[333]

Afortunadamente, esta tesis fue objeto de denuncia relativa a la contradicción de tesis 360/2013 del Pleno de la Suprema Corte de Justicia de la Nación, de la que derivó la tesis jurisprudencial P./J. 1/2015 (10a.) de título y subtítulo: "PRINCIPIO DE INTERPRETACIÓN MAS FAVORABLE A LA PERSONA. ES APLICABLE RESPECTO DE LAS NORMAS RELATIVAS A LOS DERECHOS HUMANOS DE LOS QUE SEAN TITULARES LAS PERSONAS MORALES."

Efectivamente existen derechos que solamente pueden ser de las personas físicas como:

1) Derecho a la Dignidad Humana.[334]
2) Derecho al agua, a la salud, a la dignidad, a la integridad física, a la vida, la protección de la familia, la libertad personal, la libertad de tránsito, al medio ambiente sano, culturales, alimentos.[335]

---

[332] TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL. LOS ARTÍCULOS 3o., FRACCIÓN II, Y 18, FRACCIÓN II, DE LA LEY FEDERAL RELATIVA, NO VIOLAN LA GARANTÍA DE IGUALDAD, AL TUTELAR EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES SÓLO DE LAS PERSONAS FÍSICAS. Tesis: 2a. XCIX/2008, Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XXVIII, julio de 2008, p. 549.

[333] DERECHOS HUMANOS. LAS PERSONAS MORALES NO GOZAN DE SU TITULARIDAD. Tesis: VII.2o.A.2 K (10a.),
Semanario Judicial de la Federación y su Gaceta, Décima Época, t. 3, marzo de 2013, p. 1994.

[334] DERECHO A LA DIGNIDAD HUMANA. ES CONNATURAL A LAS PERSONAS FÍSICAS Y NO A LAS MORALES. Tesis: VI.3o.A. J/4 (10a.), Semanario Judicial de la Federación y su Gaceta, Décima Época, t. 3, agosto de 2013, p. 1408.

[335] PERSONAS MORALES. CARECEN DE INTERÉS LEGÍTIMO EN EL JUICIO DE AMPARO PARA DEFENDER DERECHOS FUNDAMENTALES DE LOS QUE CAREZCAN, POR NO SER COMPATIBLES CON SU NATURALEZA. Tesis: I.18o.A.36 K (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. III, abril de 2021, p. 2205.

3) Derecho a la alimentación.[336]
4) Integridad Física.[337]

No obstante, al amparo del nuevo diseño constitucional en materia de derechos humanos, a las personas morales se les reconoce como "sujetos titulares de tales derechos, en lo que les resulte aplicable."[338]

De tal manera que "el artículo 1o. de la Constitución Política de los Estados Unidos Mexicanos, al disponer que en los Estados Unidos Mexicanos todas las personas gozarán de los derechos humanos reconocidos en dicha Constitución y en los tratados internacionales de los que el Estado Mexicano sea parte, así como de las garantías para su protección, no prevé distinción alguna, por lo que debe interpretarse en el sentido de que comprende tanto a las personas físicas, como a las morales, las que gozarán de aquellos derechos en la medida en que resulten conformes con su naturaleza y fines."[339]

Entonces se puede inferir que, si bien es cierto que existen derechos inherentes y únicos a las personas físicas, también lo es que con la modificación en materia de Derechos Humanos, casuísticamente se deberá analizar cuáles derechos humanos podrían tener las personas morales. En este sentido podría decirse que las personas morales pueden tener determinados tipos de datos que se pueden equiparar, a los de las personas físicas, ya que, de su falta de cuidado, podrían caer en riesgo en su uso.

Sobre la parte de proteger derechos de las personas morales equiparables a los personales; la ministra en retiro Margarita Luna Ramos comenta que el contenido del derecho a la intimidad y a la vida privada "puede extenderse a cierta información de las personas jurídicas colectivas, en tanto que también cuentan con determinados espacios de protección ante cualquier intromisión arbitraria por parte de terceros, respecto de información económica, comercial o relativa a su identidad que, de revelarse, pudiera anular o menoscabar su libre y buen desarrollo."[340]

---

[336] ALIMENTACIÓN. CONSTITUYE UN DERECHO HUMANO RECONOCIDO, POR REGLA GENERAL, EN FAVOR DE LAS PERSONAS FÍSICAS Y NO DE LAS MORALES. Tesis: 2a. XXXVI/2017 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. II, marzo de 2017, p. 1381.

[337] PERSONAS MORALES. LA TITULARIDAD DE LOS DERECHOS FUNDAMENTALES QUE LES CORRESPONDE DEPENDE DE LA NATURALEZA DEL DERECHO EN CUESTIÓN, ASÍ COMO DEL ALCANCE Y/O LÍMITES QUE EL JUZGADOR LES FIJE. Tesis: P. I/2014 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. I, febrero de 2014, p. 273.

[338] PERSONAS MORALES. AL RECONOCÉRSELES COMO TITULARES DE DERECHOS HUMANOS PUEDEN ACUDIR AL JUICIO DE AMPARO EN EL NUEVO SISTEMA CONSTITUCIONAL (REFORMAS CONSTITUCIONALES PUBLICADAS EN EL DIARIO OFICIAL DE LA FEDERACIÓN DE 6 Y 10 DE JUNIO DE 2011). Tesis: VII.2o.C. J/2 (10a.), Semanario Judicial de la Federación y su Gaceta, Décima Época. t. 3, abril de 2013, p. 1902.

[339] PRINCIPIO DE INTERPRETACIÓN MÁS FAVORABLE A LA PERSONA. ES APLICABLE RESPECTO DE LAS NORMAS RELATIVAS A LOS DERECHOS HUMANOS DE LOS QUE SEAN TITULARES LAS PERSONAS MORALES. Tesis: P./J. 1/2015 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. I, marzo de 2015, p. 117.

[340] Luna Ramos, Margarita, *Derecho de las personas morales a la protección de datos equiparables*

Este criterio fue generado por la Suprema Corte de Justicia, en la tesis jurisprudencial P II/2014 que por la importancia se transcribe a continuación:

> PERSONAS MORALES. TIENEN DERECHO A LA PROTECCIÓN DE LOS DATOS QUE PUEDAN EQUIPARARSE A LOS PERSONALES, AUN CUANDO DICHA INFORMACIÓN HAYA SIDO ENTREGADA A UNA AUTORIDAD.[341]
>
> El artículo 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos reconoce el derecho a la protección de datos personales, consistente en el control de cada individuo sobre el acceso y uso de la información personal en aras de preservar la vida privada de las personas. En ese sentido, el derecho a la protección de datos personales podría entenderse, en primera instancia, como una prerrogativa de las personas físicas, ante la imposibilidad de afirmar que las morales son titulares del derecho a la intimidad y/o a la vida privada; sin embargo, el contenido de este derecho puede extenderse a cierta información de las personas jurídicas colectivas, en tanto que también cuentan con determinados espacios de protección ante cualquier intromisión arbitraria por parte de terceros respecto de cierta información económica, comercial o relativa a su identidad que, de revelarse, pudiera anular o menoscabar su libre y buen desarrollo. Por tanto, los bienes protegidos por el derecho a la privacidad y de protección de datos de las personas morales, comprenden aquellos documentos e información que les son inherentes, que deben permanecer ajenos al conocimiento de terceros, independientemente de que, en materia de transparencia e información pública, opere el principio de máxima publicidad y disponibilidad, conforme al cual, toda información en posesión de las autoridades es pública, sin importar la fuente o la forma en que se haya obtenido, pues, acorde con el artículo 6o., en relación con el 16, párrafo segundo, constitucionales, la información entregada a las autoridades por parte de las personas morales, será confidencial cuando tenga el carácter de privada por contener datos que pudieran equipararse a los personales, o bien, reservada temporalmente, si se actualiza alguno de los supuestos previstos legalmente.

Lo anterior significa que la titularidad de los derechos fundamentales que les llegase a corresponder a las personas morales dependerá del derecho en cuestión, debiendo determinar el juzgador si un derecho le corresponde o no, en cada caso concreto, “como ocurre con el derecho a la protección de datos personales o a la libertad ideológica.”[342]

Por ejemplo, en una auditoría ambiental, la autoridad administrativa en uso de sus

---

a los personales, [en línea], México, El Universal, Secc. Opinión, 12 de mayo de 2020, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://www.eluniversal.com.mx/opinion/margarita-luna-ramos/derecho-de-las-personas-morales-la-proteccion-de-datos-equiparables-los*

[341] Tesis: P. II/2014 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. I, febrero de 2014, p. 274.

[342] Tesis: P. I/2014 (10a.) *op. cit.*

facultades de verificación, podría solicitar diferente información a una empresa particular. No obstante, los tribunales han interpretado que en el caso de auditorías ambientales, los poderes públicos competentes deben operar de la siguiente forma:

> 2) Abstenerse de otorgar, junto con la información medioambiental, datos confidenciales, secretos y privados de las empresas auditadas, pues ello implicaría violación irreversible a sus derechos constitucionales;
> 3) Excluir de la información pública medioambiental, la información empresarial de carácter privado;
> 4) Negar información secreta, confidencial y privada de la empresa auditada.[343]

Finalmente, las personas morales, como tales, "sí cuentan con determinados espacios, como su domicilio y sus comunicaciones, o bien, con ciertos datos económicos, comerciales o inherentes a su identidad que, de suyo, sí deben estar protegidos frente a intromisiones ilegítimas, por tanto, podemos afirmar que los bienes que tutelan o protegen los derechos a la intimidad o privacidad y de protección de datos personales, en sentido amplio, pueden comprender, en tanto no se aleja ni se opone a esa tutela, a aquellos documentos e información de las personas jurídicas colectivas que escapan al conocimiento de terceros."[344]

La complejidad en el estudio de los datos personales ha hecho que el propio Poder Judicial de la Federación emita múltiples interpretaciones en materia de Protección de Datos Personales y otros conceptos relacionados; criterios que se han ido actualizando con el devenir del tiempo y que seguramente irán formando una nueva doctrina, un nuevo "*corpus iuris*" en materia de protección de datos personales y tal vez, modificaciones a la legislación con el correspondiente evolución y entendimiento de esta institución.[345]

Visto lo anterior, a continuación, se hará el estudio de los datos personales; por una parte, de los sujetos obligados, y por la otra, en posesión de particulares.

4.1. En Posesión de Sujetos Obligados

Sin lugar a dudas, el empleo de datos personales va enlazado o relacionado con el derecho de acceso a la información; sin embargo, conviene iniciar diferenciando

---

[343] DERECHO A LA INFORMACIÓN MEDIOAMBIENTAL. SU RESPETO TRATÁNDOSE DE LAS SOLICITUDES DE DATOS SOBRE AUDITORÍAS AMBIENTALES PRACTICADAS A EMPRESAS PRIVADAS. Tesis: 2a. LXXIII/2010, Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XXXII, agosto de 2010, p. 461.

[344] CONTRADICCIÓN DE TESIS 56/2011. Registro digital: 24817, Gaceta del Semanario Judicial de la Federación. Décima Época, t. I, enero de 2014, p. 5.

[345] Suprema Corte de Justicia de la Nación, *Criterios del Poder Judicial de la Federación en materia de Protección de Datos Personales y otros conceptos relacionados*, [en línea], México, SCJN, 2da ed, 2018, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://www.scjn.gob.mx/sites/default/files/pagina_transparencia/documento/2018-11/CriteriosPJF_Proteccion_Datos_2a_Ed_Digital_2018.pdf*

estos dos derechos, como se aprecia en el siguiente cuadro:[346]

Derecho de acceso a la información pública	**Derecho a la protección de datos personales**
El derecho de acceso a la información pública garantiza la participación democrática de los ciudadanos.	El derecho a la protección de datos personales implica el poder de disposición y control sobre sus datos personales y, en consecuencia, confiere al titular una serie de derechos, acceso, rectificación, cancelación y oposición, a partir de ese poder de disposición y control.
Le permite al individuo acceder a la información que obra en los archivos de los poderes públicos siempre que dicha información no se encuentre clasificada como reservada o confidencial.	Le confiere al individuo la facultad de acceder a los datos personales que sobre su persona obran en poder de los poderes públicos, así como rectificarlos, cancelarlos y oponerse a que sean tratados.
No limita el ejercicio del derecho de protección de datos personales salvo en casos excepcionales, por ejemplo, causas de interés público.	Limita el ejercicio del derecho de acceso a la información pública, salvo casos excepcionales, por ejemplo, causas de interés público.

La LGPDPPSO indica prácticamente los mismos sujetos obligados que la LGTAIP con excepción de 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.

De lo anterior destaca que estas figuras, son sujetos obligados para efectos de transparencia, pero actúan como particulares y la protección de datos personales la harán de acuerdo con la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP). Es decir, que utilizarán el SIPOT[347] para cumplimiento de obligaciones de transparencia; pero en caso de datos personales, lo harán de acuerdo con su aviso de privacidad en términos de la LFPDPPP. Asimismo, al tratarse de una ley general, tampoco serán sujetos obligados en términos de las legislaciones de protección de datos personales estatales.

[346] *Cfr.* INAI, *Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Manual del Participante*, [en línea] México, INAI, 2017, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://cevinai-snt.inai.org.mx/repositorio/manuales/m_lgpdppso.pdf* p. 11.
[347] Sistema de Portales de Obligaciones de Transparencia.

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.[348]

La Ley maneja diversos conceptos y figuras clave, entre los conceptos clave destacan los siguientes:

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.

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.

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

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.
Asimismo, dentro de las figuras clave se encuentran las siguientes:

Titular: La persona física a quien corresponden los datos personales.

---

[348] Del Pilar Gutiérrez Paulina, *Capítulo I, De los derechos de Acceso, Rectificación, Cancelación y Oposición*, en Solange Maqueo, María, Coord. “Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Comentada”, [en línea], México, INAI, 2018, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://transparencia.guanajuato.gob.mx/bibliotecadigital/normatividad/Ley_General_de_Proteccion_de_Datos_Personales_en_Posesion_de_Sujetos_Obligados_comentada.pdf* p. 43.

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

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.

El tratamiento de datos personales que realicen las unidades administrativas deberá cumplir con los principios, deberes y obligaciones que prevé la LGPDPPSO, para lo cual este programa establecerá el marco de trabajo mínimo que se deberá seguir para alcanzar dicho objetivo.

Para ello, se identificarán las obligaciones que se deberán cumplir en todos los tratamientos de datos personales que realicen las unidades administrativas, de acuerdo con lo que establece la LGPDPPSO y los Lineamientos Generales, y según el ciclo de vida de los datos personales

Asimismo, el sujeto obligado procurará la adopción de mejores prácticas para la protección de datos personales, en aquellos tratamientos que así lo permitan y según el nivel de madurez que exista.

Para que esto pueda ser posible el INAI publicó en 2018 el Programa de Protección de Datos, (documento orientador), donde se indica el ciclo de vida de los datos personales, como se aprecia en el siguiente cuadro:[349]

[349] INAI, *Programa de Protección de Datos. Documento Orientador*, México, INAI, 2018, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://home.inai.org.mx/?page_id=3420* p. 10.

Imagen: Ciclo de vida de los datos personales.
Tomada de: INAI, *Programa de Protección de Datos. Documento Orientador*, México, INAI, 2018, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://home.inai.org.mx/?page_id=3420*, p. 10.

Ahora bien, el pasado 26 de enero de 2018, se publicó en el DOF el Programa Nacional de Protección de Datos Personales (PRONADATOS). El desarrollo del PRONADATOS, 2018-2022, se enmarca en los trabajos que realiza el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (SNT) y tiene un alcance nacional, enfocado únicamente a las instancias de gobierno.

El PRONADATOS es el principal instrumento que tiene el SNT para definir y coordinar las bases de la política pública de protección de datos personales en el país, dentro del sector público. Para ello, se auxilia de una estructura de política pública que incluye la identificación de problemáticas y el diseño de objetivos y acciones a las cuales se les dará seguimiento y en su momento se evaluarán sus resultados. Los propios lineamientos disponen de instrumentos adicionales, denominados rutas de implementación, que deberán elaborarse cada año por parte de los integrantes del SNT para la ejecución de este Programa. Al respecto cabe indicar que los integrantes que conforman al SNT son los Organismos Garantes de las Entidades Federativas, el INAI y las siguientes instancias federales: la Auditoría Superior de la Federación (ASF), el Instituto Nacional de Estadística y Geografía (INEGI) y el Archivo General de la Nación (AGN).

Este documento se elabora en cumplimiento de lo establecido en la Ley General de

Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), en particular el artículo 12 que dota al SNT del objetivo de diseñar un Programa Nacional de Protección de Datos Personales, y al artículo sexto transitorio que determina que el Sistema Nacional deberá emitir este Programa y publicarlo en el Diario Oficial de la Federación, a más tardar en un año a partir de la entrada en vigor de la LGPDPPSO.

El objetivo del PRONADATOS, en el agregado, es fortalecer las instituciones vinculadas con la protección de datos personales para generar un beneficio palpable en la población sobre su tratamiento de datos personales en el país. Entre sus objetivos en el corto plazo y mediano plazo se encuentran:[350]

- Impulsar el cumplimiento gradual de la LGPDPPSO a partir de acciones y estrategias prioritarias.
- Impulsar el fortalecimiento institucional y presupuestario de los organismos garantes para la protección de los datos personales.
- Identificar sectores y áreas relevantes donde la protección de datos personales en el país generará un beneficio y trascendencia pública y social.

En este sentido, la LGPDPPSO se distingue por prever:[351]

- Los conceptos, figuras y principios que regulan y en los que se basa el desarrollo del derecho a la protección de datos personales, de acuerdo con los estándares nacionales e internacionales en la materia, como son principios, deberes, derechos de acceso, rectificación, cancelación y oposición (derechos ARCO), portabilidad de los datos personales régimen de transferencias, entre otros.
- Los estándares mínimos e imprescindibles que permitan uniformar el derecho a la protección de datos personales en el país en el sector público federal, estatal y municipal.

En el ámbito estatal, son las entidades federativas las encargadas de regular la protección de datos personales en posesión de autoridades o entes públicos estatales, por medio de sus leyes locales armonizadas con la LGPDPPSO.

Con el fundamento de la LGPDPPSO y las leyes estatales en la materia se sientan las bases para que cualquier persona en nuestro país esté segura de:

- Que sus datos personales sean utilizados y cuidados bajo las mismas reglas en el ámbito público en los tres órdenes de gobierno;
- Que pueda solicitar a cualquier autoridad gubernamental el acceso, la rectificación, cancelación y oposición de sus datos personales;
- Que pueda denunciar el uso indebido de sus datos personales por instituciones públicas;

[350] *Programa Nacional de Protección de Datos Personales (PRONADATOS)*, [en línea] DOF: 26/01/2018.
[351] *Ídem*.

- Que sus datos personales sean comunicados a terceros sólo con su consentimiento, conforme a las reglas establecidas en la LGPDPPSO y las leyes estatales en la materia; y
- Que cuenta con una serie de mecanismos a su favor para el caso de que le sea vulnerado o restringido su derecho a la protección de datos personales en el ámbito público.

El PRONADATOS es un instrumento de política pública que atiende los elementos de una planeación estratégica adecuada para encauzar las acciones que en materia de protección de datos personales se desarrollen en el sector público a nivel nacional.

El PRONADATOS maneja una serie de perspectivas de 2018 hasta el 2037 de la siguiente forma:

Dónde estamos 2018-2020 (Etapa 1 PRONADATOS)	Dónde estaremos 2020-2022 (Etapa 2 PRONADATOS)	Hacia dónde vamos 2022-2026 (SEGUNDO PRONADATOS)	Qué aspiramos 2037 (20 años de la LGPDPPSO)
Se establecen las condiciones institucionales que permitan que los integrantes del SNT cumplan sus obligaciones establecidas en la LGPDPPSO y las legislaciones locales.	Los integrantes del SNT cumplen a cabalidad las obligaciones que les ha establecido la LGPDPPSO.	Los organismos garantes se consolidan como instituciones capaces de garantizar la protección de los datos personales de las y los titulares. Y los integrantes federales del SNT (AGN, ASF e INEGI) son parámetros de buenas prácticas en la materia.	El SNT se consolida como un mecanismo comprobado y reconocido para la generación de una garantía efectiva y homogénea del derecho a la protección de los datos personales para toda la población del país.
Se comienzan esfuerzos generalizados para incrementar el conocimiento del derecho y su ejercicio entre la población.	Hay un incremento en el porcentaje de personas que identifica la legislación en materia de protección de datos personales, así como en el	La población incrementa el ejercicio de su derecho a la protección de datos personales para proteger su privacidad y la de sus familiares.	La mayoría de la población identifica los mecanismos que le permiten ejercer su derecho a la protección de datos personales.

Dónde estamos 2018-2020 (Etapa 1 PRONADATOS)	Dónde estaremos 2020-2022 (Etapa 2 PRONADATOS)	Hacia dónde vamos 2022-2026 (SEGUNDO PRONADATOS)	Qué aspiramos 2037 (20 años de la LGPDPPSO)
	conocimiento de las instituciones encargadas de la garantía de este derecho.		
Se impulsa el cumplimiento de los responsables del ámbito público en los distintos niveles de gobierno en materia de sus obligaciones en materia de protección de datos personales.	Se evalúa a todos los responsables del ámbito público en el cumplimiento de sus obligaciones en materia de protección de datos personales.	Las instituciones públicas que manejan una mayor cantidad de datos personales lo hacen cumpliendo con lo dispuesto en la LGPDPPSO.	La gestión de la seguridad de la información en todos los niveles del sector público está internalizada y es aplicada constante y eficientemente por los servidores públicos.
Se generan líneas base para la medición de los aspectos más relevantes de la protección de datos personales en el sector público.	Se desarrolla una serie de instrumentos y mecanismos que permiten contar con la información necesaria para la evaluación del estado que guardan los principales aspectos de la protección de datos en el sector público del país.	Se cuenta con análisis de las fuentes de información que permiten dar cuenta de los cambios generados por las acciones del PRONADATOS.	La generación de información, su conversión en conocimiento y su integración en la toma de decisiones en materia de protección de datos personales es una rutina institucionalizada en el Estado mexicano.

Además de la Ley General, el pasado 26 de enero de 2018, se publicaron en el DOF, los Lineamientos Generales de Protección de Datos Personales para el Sector Público, los cuales tienen por objeto desarrollar las disposiciones previstas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, (LGPDPPSO) en lo relativo al ámbito Federal.

Dado que la protección de datos personales en posesión de sujetos obligados se volvió una facultad concurrente, las entidades federativas regularán sus propias

leyes alineadas por supuesto a la Ley General, y emitirán sus propios Lineamientos. Asimismo, los otros sujetos obligados como el poder judicial, el legislativos, los órganos constitucionales autónomos, universidades con autonomía, también han emitido diversos lineamientos en materia de protección de datos personales.
Dado también que los datos personales que sean tratados pueden implicar el tratamiento de datos personales de menores, el responsable del tratamiento de datos personales deberá privilegiar el interés superior de las niñas, niños y adolescentes en términos de las disposiciones previstas en la Ley General de los Derechos de Niñas, Niños y Adolescentes.

4.1.1.1 Principios de protección de datos personales

La Ley General en su artículo 16 dispone que el responsable deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

Ahora bien, a juicio del que esto escribe, y basado en la experiencia de dar diferentes cursos a sujetos obligados federales y locales, que la aplicación de los principios si bien son importantes todos, en su aplicación es como si fueran una serie de capas como se muestra en el siguiente cuadro:

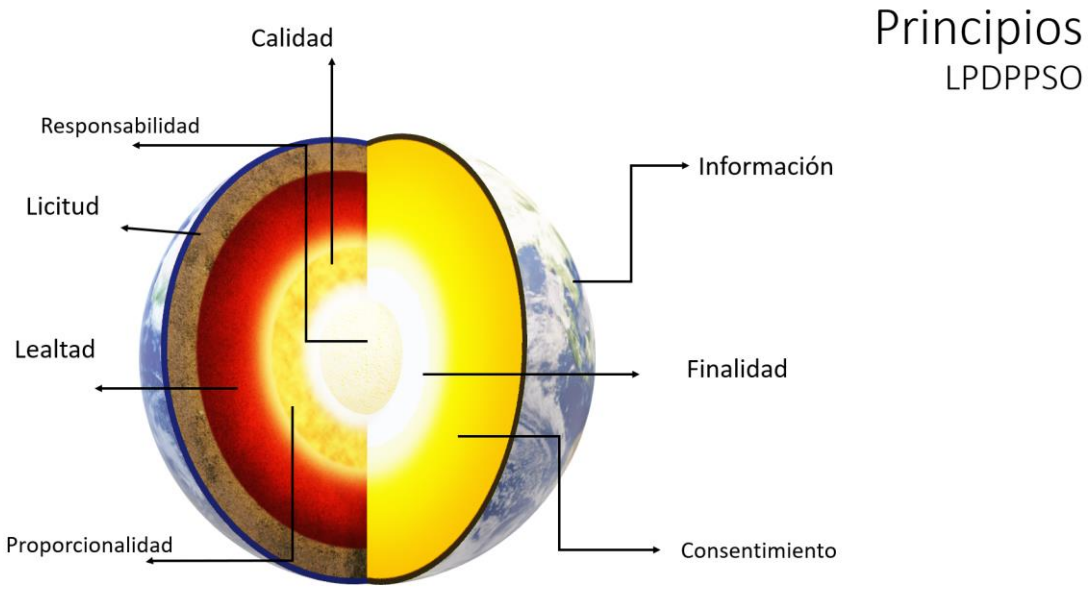


Imagen: Principios de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
Fuente: Elaboración propia.

Como se puede apreciar, la capa externa, es decir, la que podríamos ver todos es la que viene con el principio de información, que vendría a materializarse con el Aviso de Privacidad, el cual es el principal instrumento con que los sujetos obligados

nos indican como van a realizar el tratamiento de los datos personales.

A su vez, el núcleo de estos principios es el correspondiente al principio de responsabilidad, el cual corresponde a la forma en que de manera interna el sujeto obligado cuida, establece las medidas de seguridad de datos personales.

Además, en el cumplimiento de estos principios, se deben cuidar los deberes de seguridad y confidencialidad en el tratamiento de datos personales.

En 2018, el INAI publicó en su sitio web la guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, mismo que se enlaza con el Programa de Protección de Datos, el cual apoya también con el cumplimiento de los principios en materia de protección de datos, así como con el cumplimiento de otras obligaciones dependiendo la fase del ciclo de vida de datos personales, para lo cual se elabora el siguiente cuadro:[352]

Obligaciones relevantes en la etapa de **OBTENCIÓN** de los datos personales	Obligaciones relevantes en la etapa de **USO** de los datos personales	Obligaciones relevantes en la etapa de **ELIMINACIÓN** de los datos personales
Principio de Licitud	Principio de Finalidad	Supresión de los Datos Personales (Calidad)
Principio de Lealtad	Principio de Calidad	
Principio de Información (Aviso de Privacidad) Tratamiento de Datos Personales Sensibles	Relación con los encargados	
Medidas Compensatorias	Manejo del cómputo en la nube	
Principio de Consentimiento Consentimiento de menores de edad y personas en estado de interdicción o incapacidad declarada conforme a la Ley Cumplimiento del Interés Superior de los menores de edad	Tratamiento de las Transferencias	
Principio de Proporcionalidad	Atención de solicitudes de ejercicios de Derechos	

[352] Basado en INAI, *Programa de Protección de Datos, Documento Orientador*, *op cit*.

	ARCO Atención de opciones de Portabilidad	
Principio de Responsabilidad		
Impacto en la Protección de Datos Personales		
Funciones del Comité de Transparencia (Capacitación)		
Funciones de la Unidad de Transparencia		

Dicho lo anterior, a continuación, se abordarán cada uno de los principios que marca la Ley General.

4.1.1.2 Principio de Licitud.

Podría decirse que este es un principio global; es decir, que su cumplimiento implica cumplir con todos los demás principios de la ley. En términos generales licitud es derivado de ley, lo cual significa que se cumple con este principio cuando el responsable cumple con la normatividad aplicable al tratamiento de datos personales, dentro de la cual se tiene la siguiente:

1) Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
2) Ley General de Archivos
3) Ley General de los Derechos de Niñas, Niños y Adolescentes
4) Lineamientos Generales de Protección de Datos Personales para el Sector Público
5) Acuerdo mediante el cual se aprueba la adición de un Título Décimo a los Lineamientos Generales de Protección de Datos Personales para el Sector Público
6) Criterio de Interpretación 10-17 Cuentas Bancarias y CLABE Interbancaria de personas físicas y Morales privadas.
7) Criterio de interpretación 15-17 Fotografía en título o cédula profesional es de acceso público.
8) Criterio de Interpretación 01-18 Entrega de datos personales a través de medios electrónicos.
9) Criterio de Interpretación 03-18 Fallecimiento del titular previo a la entrada en vigor de la Ley General.
10) Criterio de Interpretación 04-18 Resolución del CT en cado de improcedencia de derechos ARCO.
11) Criterio de Interpretación 05-18 Improcedencia en el envío a domicilio de datos personales.
12) Criterio de Interpretación 01-19 Datos de identificación del representante o apoderado legal.
13) Criterio de Interpretación 08-19 Razón Social y RFC de personas morales.

14) Criterio de Interpretación 09-19 Edad o fecha de nacimiento de los servidores públicos es información pública.

Cabe señalar que otros sujetos obligados tanto de índole federal como estatal tienen otras normas secundarias, por ejemplo:

Sujeto Obligado	Norma
Cámara de Diputados del Congreso de la Unión	Reglamento de Transparencia, Acceso a la Información Pública y Protección de Datos Personales de la Cámara de Diputados del Congreso de la Unión Guía para la elaboración del Aviso de Privacidad Integral y Simplificado en la Cámara de Diputados
Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Puebla	Guía para la elaboración de Avisos de Privacidad en el Sector Público
Instituto Nacional Electoral	Reglamento del Instituto Nacional Electoral en Materia de Protección de Datos Personales Guía para elaborar el Aviso de Privacidad
Suprema Corte de Justicia de la Nación	Acuerdo del Comité Especializado de Ministros Sustanciación de Recursos de Revisión de Datos Personales en la SCJN Acuerdo General 11-2017 Protección del Nombre en Instrumentos Jurisdiccionales Acuerdo General II-2020 Lineamientos de Seguridad Sanitaria en la SCJN Durante la Emergencia Sanitaria Causada por el Virus SARS-COV2 (COVID-19)
Universidad Nacional Autónoma de México	Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México (2016) Lineamientos para la Protección de Datos Personales en posesión de la Universidad Nacional Autónoma de México

Sujeto Obligado	Norma
INEGI	Lineamientos de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Instituto Nacional de estadística y Geografía. (2021)
Comisión Nacional de Derechos Humanos	Documento de Seguridad (de Datos Personales)
Banco de México	Norma Administrativa Interna Gestión de la Información. Criterios para establecer y mantener el sistema de Gestión de Seguridad de Datos Personales. Política interna de gestión y tratamiento de datos personales. Políticas y Programas de Protección de Datos Personales.

Adicionalmente a la normatividad obligatoria, existen otras guías y normas que apoyan en el cumplimiento del principio de licitud que han sido emitidas por el INAI como:

a) Recomendaciones para los sujetos obligados en la designación del oficial de protección de datos personales.
b) Guía para la elaboración del Aviso de Privacidad en el área de Recursos Humanos. Sector Público.
c) Recomendaciones para el manejo de incidentes de seguridad de datos personales.
d) Recomendaciones para reconocer las principales amenazas a los datos personales a partir de la valoración respecto al riesgo.
e) Guía breve para sujetos obligados para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales.
f) Conformidad de contratos de adhesión de servicios de cómputo en la nube vs los criterios mínimos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales.
g) Guía para el tratamiento de datos biométricos.
h) Recomendaciones sobre protección de datos personales contenidos en la Credencial para Votar.
i) Documento orientador para la elaboración del Programa de Protección de Datos Personales.
j) Anexos del Documento orientador para la elaboración del Programa de Protección de Datos Personales.

k) El ABC del Aviso de Privacidad (Sector Público).
l) Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
m) Recomendaciones para orientar el debido tratamiento de datos personales en el registro de control de acceso a edificios e instalaciones de los sujetos obligados.
n) Guía para instrumentar medidas compensatorias en el sector público.
o) Recomendaciones sobre el tratamiento de los datos personales en los expedientes clínicos de las Instituciones de Salud Pública.
p) Guía para la protección de datos personales con perspectiva de gestión documental y archivos.
q) Recomendaciones para personas titulares de los datos personales en el ámbito laboral para el sector público.
r) Guía de protección de datos personales para las personas titulares en situaciones de emergencia.
s) Recomendaciones para los sujetos obligados respecto a la aplicación del principio de proporcionalidad en el tratamiento de los datos personales recabados.
t) El ABC de los esquemas de mejores prácticas en materia de protección de datos personales.

4.1.1.3 Principio de lealtad

El artículo 19 de la LGPDPPSO dispone 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.
Por su parte el artículo 11 de los Lineamientos indica que lo que dispone el artículo 19 de la LGPDPPSO implica:

1) Por medios engañosos o fraudulentos aquellos que el responsable utilice para tratar los datos personales con dolo, mala fe o negligencia.
2) Que el responsable privilegia los intereses del titular cuando el tratamiento de datos personales que efectúa no da lugar a una discriminación o trato injusto arbitrario contra este.
3) Por expectativa razonable de privacidad, la confianza que el titular ha depositado en el responsable respecto a que sus datos personales serán tratados conforme a los señalado en el aviso de privacidad y en cumplimiento a las disposiciones previstas en la LGPDPPSO.

4.1.1.3 Principio de Consentimiento

Este principio tiene que ver con la forma en que el titular pueda manifestar el consentimiento para el tratamiento de los datos personales.
Existen dos formas para manifestarlo tal como se muestra en el siguiente cuadro:[353]

Consentimiento tácito	Consentimiento Expreso

[353] Artículo 21, LGPDPPSO.

Se presenta cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario.	Se presenta cuando la voluntad del titular se manifieste de forma verbal, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología.

Este es tal vez, el principio más complejo en cuanto a su cumplimiento y forma de probar que se ha obtenido, ya que implican formas de obtenerlo, si existen cuestiones obligadas de que sean expreso y por escrito, excepciones al consentimiento, consentimiento en caso de menores y privilegio del interés superior del menor.

Ante ello, tanto la Ley, los lineamientos y el documento orientador, dedican bastante a las formas de obtener el consentimiento, y que aun a la fecha, es uno de los principios más difíciles de entender y de cumplir.

Uno de los problemas prácticos es la parte que indica el artículo 15 de los Lineamientos el cual en su último párrafo menciona que el responsable deberá documentar la puesta a disposición del aviso de privacidad; esto es así porque pareciera que el consentimiento está atado a la puesta a disposición del aviso de privacidad cuando a juicio del que esto escribe; son cosas diferentes.

Es decir, por una parte, el hecho de poner a puesta el aviso de privacidad es parte de dar cumplimiento al principio de información, por medio del cual el responsable comunica la forma de dar tratamiento a los datos personales, mientras que en el consentimiento está ligado con el principio de finalidad que consiste en manifestar el para qué se emplean los datos personales; y más en el caso de que estos sean sensibles o que involucren datos de menores de edad.

Por lo anterior, el consentimiento, va enlazado solamente en cuanto a la finalidad por lo que hace al consentimiento para el tratamiento de datos sensibles o de menores de edad, y por otra parte en la aceptación del aviso de privacidad.

Otro problema es con el mismo último párrafo del artículo 15 de los Lineamientos en relación con el consentimiento verbal; el cual se presenta cuando lo externe oralmente de manera presencial o mediante el uso de cualquier otra tecnología. El problema estriba en la interpretación de que ese último párrafo del artículo 15 de los Lineamientos está en la parte de consentimiento tácito, pero a la vez el consentimiento puede ser verbal; no obstante, el responsable deberá documentar la puesta a disposición del aviso de privacidad.

Este problema no ocurre por lo que hace al tratamiento de datos sensibles, en cuyo caso el consentimiento deberá ser expreso y por escrito. En este caso lo óptimo es obtener en un mismo acto una leyenda donde se acepta el aviso de privacidad y el consentimiento de datos personales de manera general (en ese orden: 1) Aceptar aviso de privacidad, y 2) Otorgar consentimiento); y, dependiendo el caso, solicitar

el consentimiento para tratamiento de datos sensibles de acuerdo con las finalidades que se indiquen en el Aviso de Privacidad.

Dada la complejidad que se tiene con este principio de consentimiento, el documento orientador del programa de protección de datos, sugiere diferentes vías de comprobación de este principio siendo las siguientes:
Cumplimiento del consentimiento:[354]

Comprobación:

	Sí	No
1. Se han identificado las finalidades para las cuales se requiere el consentimiento.	☐	☐
2. Se ha definido el tipo de consentimiento que se requiere, según el tipo de datos personales que se tratan y tomando en cuenta las disposiciones normativas que regulan el tratamiento.	☐	☐
3. Se han habilitado los mecanismos para solicitar el consentimiento expreso, en su caso.	☐	☐
4. El consentimiento se requiere después de que se da a conocer el aviso de privacidad.	☐	☐
5. Se encuentra documentada la puesta a disposición del aviso de privacidad y la obtención del consentimiento expreso, en su caso.	☐	☐
6. Las solicitudes de consentimiento se encuentran redactadas de forma tal que éste sea libre, específico e informado, y de que las solicitudes sean concisas e inteligibles, estén en un lenguaje claro y sencillo acorde con el perfil del titular, y se distingan de asuntos ajenos a la protección de datos personales, cuando ello sea necesario.	☐	☐
7. Cuando los datos personales se recaban directamente del titular, el consentimiento se solicita previo a la obtención de los datos personales y después de la puesta a disposición del aviso de privacidad.	☐	☐
8. Cuando los datos personales se recaban de manera indirecta, (i) se envía el aviso de privacidad correspondiente a los titulares; (ii) se les informa sobre los 5 días hábiles que tienen para manifestar su negativa; (iii) en caso de que se requiera el consentimiento expreso, éste se solicita y los datos personales se tratan sólo si se cuenta con el mismo.	☐	☐
9. El procedimiento interno para atención de derechos ARCO contempla lo relativo a la revocación del consentimiento.	☐	☐

Consentimiento para datos sensibles: Comprobación[355]

	Sí	No
1. El tratamiento de datos personales sensibles está debidamente justificado por las atribuciones de la unidad administrativa y el principio de necesidad.	☐	☐
2. Se tienen identificados los casos en los que se requiere el consentimiento expreso y por escrito de los titulares.	☐	☐
3. Se obtiene el consentimiento expreso y por escrito del titular.	☐	☐

[354] INAI, *Programa de Protección de Datos, Documento Orientador*, *op cit*. p. 36.
[355] *Ibidem*. p. 40.

4. Se ha verificado que el tratamiento no tenga como consecuencia discriminación para los titulares.	☐	☐

Consentimiento tomando en consideración el interés superior de los menores de edad. Comprobación[356]

	Sí	**No**
1. Se privilegia el interés superior del menor en el tratamiento de datos personales.	☐	☐
2. Se conoce la Ley General de Niñas, Niños y Adolescentes.	☐	☐
3. Se obtuvo el consentimiento del adulto en representación del menor, y se solicitó la opinión del menor, en su caso.	☐	☐

4.1.1.4 Principio de Información

Este principio se cumple principalmente con la puesta a disposición a los titulares del aviso de privacidad el cual es un "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".[357]

Este principio considero que es un principio aglutinador, esto lo comento, debido a que, por medio del aviso de privacidad, se cumplen otra serie de principios como el de finalidad, proporcionalidad, calidad, parte del de responsabilidad, consentimiento y lealtad.

De acuerdo con la Ley General son dos los tipos de aviso de privacidad con los que se deben de cumplir el Aviso Simplificado y el Aviso de Privacidad Integral (Arts. 27 y 28 respectivamente). De estos los elementos informativos que se deben colocar de acuerdo con la modalidad son los siguientes:[358]

ELEMENTO INFORMATIVO	INTEGRAL	SIMPLIFICADO
1. Denominación del responsable	✓	✓
1bis (Opcional). Abreviatura o acrónimo por el cual se identifica el responsable	✓	✓
2. Domicilio de responsable.	✓	
2 bis (opcional). Datos de Contacto	✓	
3. Datos Personales	✓	
3bis (opcional). Medios y/o fuentes de obtención de los datos personales.	✓	

[356] *Ibidem*. p. 41.
[357] Artículo 3°, fracción II, LGPDPPSO.
[358] Tomado de INAI, *Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de sujetos Obligados*, [en línea], México, INAI, 2018, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/_GuiaPrincipiosDeberes.pdf* p. 28.

4. Finalidades del tratamiento.	✓	✓
5. Transferencias que requieren consentimiento.	✓	✓
5 bis (opcional). Transferencias que no requieren consentimiento.	✓	
6. Negativa del consentimiento.	✓	✓
7. Sitio donde se podrá consultar el aviso de privacidad integral.		✓
8. Fundamento legal.	✓	
9. Derechos ARCO y Portabilidad	✓	
10. Portabilidad	✓	
11. Domicilio de la Unidad de Transparencia	✓	
12. Cambios al Aviso de Privacidad	✓	
13. Fecha de elaboración o última actualización	✓	✓
14. Características del aviso de privacidad	✓	✓

Cabe señalar que además de a Ley General, los lineamientos y el Documento Orientador, existen otros tres documentos que apoyan en el auxilio del cumplimiento de este principio, como lo son: La Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de sujetos Obligados; el ABC del aviso de privacidad. Sector Público, y el formato de autoevaluación de Avisos de Privacidad, todos publicados por el INAI.

Dentro del documento del ABC del Aviso de Privacidad existen algunas ideas que vale la pena compartir:

1) Cualquier sujeto obligado está obligado a tener aviso de privacidad.
2) Tener aviso de privacidad es independiente de que no se requiera el consentimiento del titular para el tratamiento de sus datos personales.
3) El aviso de privacidad tiene como objeto informar al titular sobre los alcances y condiciones generales del tratamiento de los datos personales.
4) No existe limitación alguna sobre el número de avisos de privacidad que como responsable requiera utilizar.
5) Existen diferentes prácticas que no deben realizarse al generar un aviso de privacidad tales como:
    a. Usar frases inexactas, ambiguas o vagas, como “entre otros”, “como por ejemplo” o “de manera enunciativa más no limitativa”.
    b. Incluir textos o frases que induzcan al titular, de manera engañosa o fraudulenta, a seleccionar una opción en específico, por ejemplo, “Le recomendamos que nos autorice el uso de su información personal sin restricción alguna, para ser más eficientes en nuestro servicio”.
    c. Incluir casillas u otros mecanismos similares que estén marcados previamente, y que obliguen a los titulares a desmarcarlos para modificar la condición ahí establecida.

d. Remitir al titular a textos o documentos que no estén disponibles, por ejemplo, a hipervínculos deshabilitados o que no contengan la información señalada.

6) Considerar al momento de elaborar el aviso de privacidad:
   a. Conocer las obligaciones y deberes como sujeto obligado del sector público.
   b. Identificar facultades o atribuciones.
   c. Identificar actividades y/o procedimientos en los que se utilizan datos personales.
   d. Identificar como se obtienen los datos personales.
   e. Identificar los fines para los que se utilizarán los datos personales, así como el tipo de datos de los que se realizará el tratamiento.
   f. Identificar las transferencias de datos personales, así como la ubicación de los remitentes; es decir, si son nacionales o extranjeros.
   g. Identificar el perfil de los titulares de los datos personales.
   h. Identificar los mecanismos para el ejercicio de los derechos ARCOP.
   i. Identificar los tipos de consentimiento que se requieren.
   j. Identificar información adicional sobre otras prácticas de privacidad.
   k. Identificar el tratamiento de datos en el marco de un sistema de Gestión.

El INAI cuenta con un Generador de Avisos de Privacidad para el sector público[359], el cual, a juicio del que esto escribe es una herramienta poco útil, ya que tan solo el cumplimiento del principio de consentimiento como este de información es demasiado amplio y complejo; por lo que esta herramienta, considero no está suficientemente desarrollada.

Así como el principio de consentimiento es muy complejo, el principio de información es sumamente elaborado por la cantidad de componentes que debe de desarrollar, como se acaba de apreciar.

Cabe señalar también que, de acuerdo con la guía para el cumplimiento de los principios y deberes, en el mismo aviso de privacidad se deberá indicar las medidas compensatorias, para dar a conocer el aviso de privacidad. Estas medidas compensatorias son mecanismos alternos para dar a conocer a los titulares el aviso de privacidad, a través de su difusión en medios de comunicación masiva en lugar de hacerlo de manera personal o directa, siempre y cuando resulte imposible dar a conocer el aviso de privacidad al titular de manera directa o bien, exija esfuerzos desproporcionados.

4.1.1.5 Principio de Proporcionalidad.

Significa realizar el tratamiento de los datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtienen

[359] Véase, INAI, *Generador de Avisos de Privacidad. Sector Público,* [en línea], México, INAI, s.a. [fecha de consulta: 4 de diciembre de 2022] Disponible en: *http://gapsectorpublico.inai.org.mx/*

los datos personales por parte de los sujetos obligados.
De acuerdo con el documento orientador, se entiende por cumplimentado este principio si:

	Sí	No
1. Se tienen identificados los datos personales que se requieren para cada una de las finalidades.	☐	☐
2. Los datos personales que se solicitan son los mínimos necesarios para cumplir con las finalidades.	☐	☐

Cabe señalar que este principio de proporcionalidad se complementa con el criterio de minimización el cual consiste en que el responsable deberá realizar esfuerzos razonables para limitar los datos personales tratados al mínimo necesario, con relación a las finalidades que motivan su tratamiento. (Art. 25 de los Lineamientos)

4.1.1.6 Principio de Finalidad

Este principio considero que va íntimamente ligado con el principio de información y el de consentimiento, aunque también podría ligarse con el de calidad, lealtad y proporcionalidad.

Se entiende por finalidad del tratamiento, el propósito, motivo o razón por el cual se tratan los datos personales.

Los datos personales sólo pueden ser tratados para cumplir con la finalidad o finalidades que hayan sido informadas al titular en el aviso de privacidad y, en su caso, consentidas por éste.

Las finalidades deben ser concretas, explicitas, licitas y legitimas:[360]

➢ Concretas: Cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión en el titular.
➢ Explícitas: Tienen lugar cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad.
➢ Lícitas: Cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones o facultades del responsable, conforme a lo previsto en la legislación mexicana y el derecho internacional que le resulte aplicable.
➢ Legítimas: Cuando las finalidades que motivan el tratamiento de los datos personales se encuentran habilitadas por el consentimiento del titular, salvo que se actualice alguna de las causales de excepción previstas en el artículo 22 de la Ley General.

[360] INAI, *Guía para cumplir con los principios y deberes de la Ley General… op. cit*. p 36.

4.1.1.6 Principio de Calidad

Este se cumple en concordancia con el artículo 23 de la Ley General y 21 de los Lineamientos; es decir, que los datos deben ser:

a) Exactos y Correctos
b) Completos
c) Actualizados

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.

Este principio se complementa con el plazo de conservación de datos y la supresión de los mismos.

El plazo de conservación varía de acuerdo con cada sujeto obligado o bien con la normatividad respectiva que fije algún plazo en particular. Servirá como referencia lo relacionado con lo que disponga la Ley General de Archivos. Por ejemplo, el artículo 37 de dicha ley dispone que el sujeto obligado deberá asegurar que se cumplan los plazos de conservación establecidos en el catálogo de disposición documental y que los mismos no excedan el tiempo que la normatividad específica que rija las funciones y atribuciones del sujeto obligado disponga, o en su caso, del uso, consulta y utilidad que tenga su información. En ningún caso el plazo podrá exceder de 25 años

Por otra parte, los lineamientos disponen que el responsable deberá establecer políticas, métodos y técnicas orientadas a la supresión definitiva de los datos personales, de tal manera que la probabilidad de recuperarlos sea mínima.

Asimismo, en el establecimiento de políticas, métodos y técnicas para la supresión de datos se deberán considerar al menos los siguientes atributos: (Art. 23 de los Lineamientos)

I. **Irreversibilidad**. Que el proceso utilizado no permita recuperar los datos personales.
II. **Seguridad y confidencialidad**. Que en la eliminación definitiva de los datos personales se consideren los deberes de confidencialidad y seguridad.
III. **Favorable al medio ambiente**. Que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten el medio ambiente.

4.1.1.7 Principio de Responsabilidad

Este principio podría decirse que es el núcleo de los principios en función que su cumplimiento es al interior del sujeto obligado.

El principio de responsabilidad significa que el responsable deberá adoptar políticas e implementar mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la Ley; así como establecer mecanismos necesarios para evidenciar dicho cumplimiento ante los titulares y el INAI.

4.1.2 Medidas de seguridad y de gestión que los sujetos obligados deben seguir

La ley y los lineamientos citados en este capítulo, disponen dos deberes principales que deben de cumplir, los cuales son los deberes de confidencialidad y seguridad.

> 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.[361]

[361] Velázquez, Andrés, *Capítulo II, De los Deberes*, en Solange Maqueo, María, *op. cit.* p. 97.

Por su parte, en la las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal publicado en el DOF el 06 de septiembre de 2021, indica que todos los proyectos de TIC que las instituciones pretendan ejecutar a través de prácticas de desarrollo, implementación propia, o a través de contrataciones, deben apegarse a un proceso de planeación estratégica alineado a las disposiciones del Plan Nacional de Desarrollo y programas que de él deriven, la Estrategia Digital Nacional, así como a la legislación en materia de desarrollo nacional, presupuesto, austeridad y transparencia.

El proceso de planeación de TIC se formaliza con la integración y registro del Portafolio de Proyectos de Tecnologías de la Información y Comunicación (POTIC).

Cuando los servicios de correo electrónico sean contratados a un proveedor, éste deberá garantizar, al menos: La suscripción de un Acuerdo de Confidencialidad respecto de la información y datos personales relacionados con los correos electrónicos y usuarios del servicio prestado, el cual deberá prevenir efectos legales durante y después de la vigencia del contrato.

Los proyectos de servicios de desarrollo o mantenimiento de software deberán incluir el diseño detallado o conceptual del aplicativo a desarrollar, que comprenda por lo menos:

a) Requerimientos del negocio;
b) Mecanismos o esquemas de seguridad de la información;
c) Políticas de privacidad y protección de datos personales, de conformidad con la legislación aplicable;
d) Alcance de los módulos;
e) Perfiles de usuario;
f) Matriz de trazabilidad;
g) Protocolos de pruebas y;
h) Mecanismos de autenticación a través de la Firma Electrónica Avanzada (e-firma), cuando resulte aplicable.

Los aplicativos de cómputo o servicios de TIC y de seguridad de la información, deberán contemplar como campo llave para su interoperabilidad, la Clave Única de Registro de Población (CURP) o el RFC al tratarse de personas físicas o el folio mercantil en el caso de personas morales y, en su caso, otros atributos que permitan realizar la autenticación electrónica correspondiente, como lo es la Firma Electrónica Avanzada (e-firma), en todos los casos, deberán preverse medidas de protección a los datos personales, de conformidad con la legislación aplicable.

Otros sujetos obligados como la Suprema Corte de Justicia de la Nación, en la parte de medidas de seguridad administrativas, ha publicado el documento intitulado

Inventario de Tratamientos de Datos Personales[362], el cual considero un extraordinario documento, el cual indica:

1) Áreas de la SCJN que recaban datos personales.
2) Listado completo de los Datos personales que recaba cada una de las áreas de la SCJN.
3) Finalidades de la obtención de los datos personales que recaban.
4) Fundamento legal de recabar los datos personales.
5) Forma de obtención de los datos personales.
6) Cargos que tienen acceso a la bace se datos (parte de la trazabilidad de datos personales)
7) Tipo de soporte en la que almacenan los datos personales.
8) Si se hacen transferencia o no.
9) Plazo de conservación.
10) Medidas del Catálogo de Disposición Documental (CADIDO 2021).
11) Si tienen aviso de privacidad *ex profeso*.
12) Medidas en tratándose de COVID-19.

Este es un documento muy bueno en cuanto a su creación y contenido; sin embargo, considero que se debería hacer mención o relacionarlo con el aviso de privacidad, o sus avisos de privacidad en su caso, de tal manera que mantengan estable el sistema de datos personales, con el fin de que no se consideren documentos aislados, sino en conjunto.

Por otra parte, la Ley General obliga a que los responsables (sujetos obligados) deberán elaborar un documento de seguridad que contenga **al menos**, lo siguiente:

1) El inventario de datos personales y de los sistemas de tratamiento.
2) Las funciones y obligaciones de las personas que traten datos personales.
3) Los análisis de riesgo y brecha.
4) El plan de trabajo.
5) Los mecanismos de monitoreo y revisión de las medidas de seguridad.
6) El programa general de capacitación.

A su vez los Órganos Garantes, han emitido una serie de recomendaciones para elaborar un documento de seguridad, por ejemplo:

SUJETO OBLIGADO	DOCUMENTO
INAI	Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales
IAP (OAXACA)	¿Qué es y cómo elaborar un Documento de Seguridad?: Guía para sujetos obligados
INFOCDMX	Guía para la elaboración del documento de seguridad

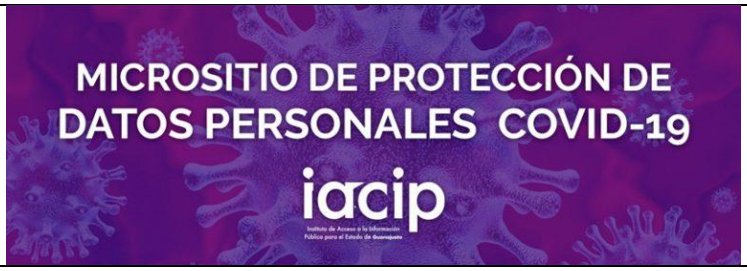
[362] Suprema Corte de Justicia de la Nación, *Inventario de tratamientos de datos personales*, [en línea] México, SCJN, 2021, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://datos-personales.scjn.gob.mx/sites/default/files/documentos-relevantes/Inventario-Tratamientos-2021-2o-Semestre.pdf*

SUJETO OBLIGADO	DOCUMENTO
ITEI (JALISCO)	Guía para elaborar un documento de seguridad
INFOEM (EDOMEX)	Lineamientos sobre medidas de seguridad aplicables a los sistemas de datos personales que se encuentran en posesión de los sujetos obligados de la Ley de Protección de Datos Personales del Estado de México

Cabe destacar que ante esta contingencia sanitaria el INAI y otros organismos garantes, se han creado micrositios sobre el cuidado de los datos personales y el COVID-19, siendo únicamente los siguientes casos:[363]

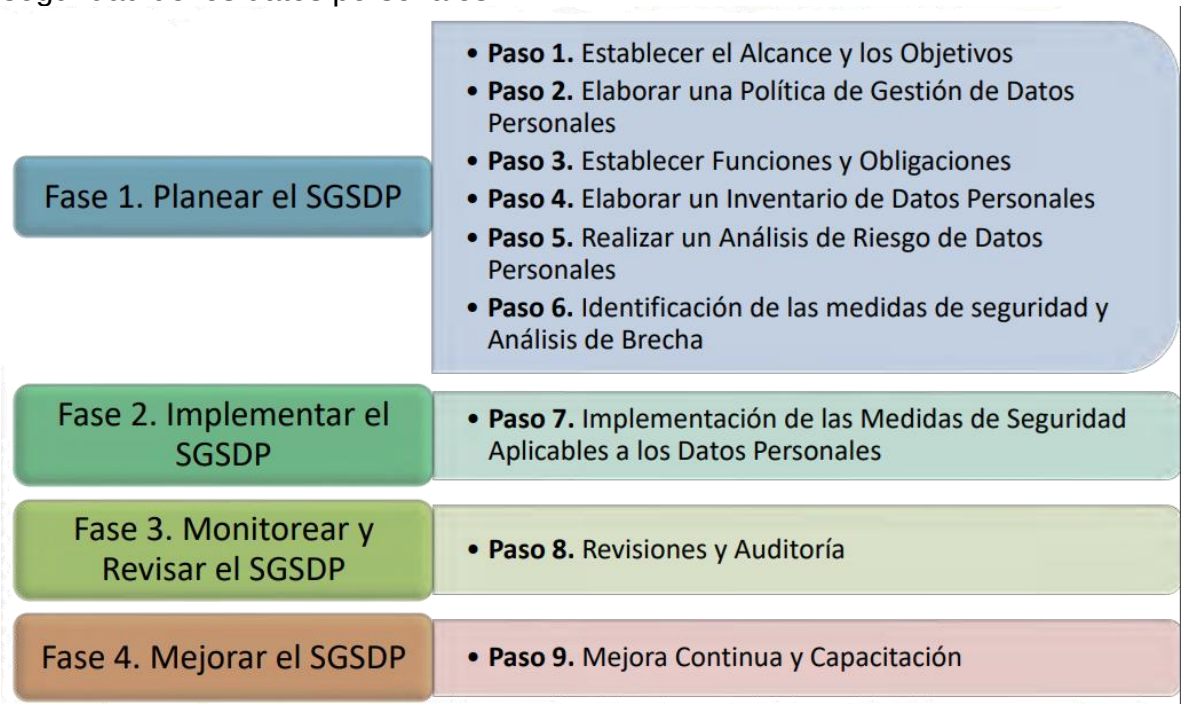
ÓRGANO GARANTE	MICROSITIO
INAI	
Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas (ITAIPCH)	
Instituto de Transparencia, Acceso a la Información, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (INFOCDMX)	
Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de	

[363] Elaboración propia a partir de la revisión de las páginas de los órganos garantes.

ÓRGANO GARANTE	MICROSITIO
México	
Instituto de Acceso a la Información Pública para el Estado de Guanajuato (IACIP)	
Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Guerrero (ITAIGro)	
Instituto Morelense de Información Pública y Estadística (IMIPE)	
Comisión Estatal para el Acceso a la Información Pública (Sinaloa)	
Instituto de Acceso a la Información Pública y Protección de Datos Personales del Estado de Tlaxcala (IAIP Tlaxcala)	

ÓRGANO GARANTE	MICROSITIO
Instituto Veracruzano de Acceso a la Información y Protección de Datos Personales (IVAI)	
Instituto Zacatecano de Transparencia y Acceso a la Información (IZAI)	

Otra parte que se tiene que contemplar es la de adoptar un Sistema de Gestión de Seguridad de Datos Personales (SGSDP), se debe hacer basado en el ciclo (PHVA) Planear-Hacer-Verificar-Actuar). En este sentido el responsable deberá implementar un sistema de gestión, mismo que funciona a través de un ciclo de mejora continua, dividido en 4 fases que consideran 9 pasos o actividades para la seguridad de los datos personales:[364]



[364] INAI, *Guía para cumplir con los principios y deberes de la Ley General… op. cit*. p 47.

Imagen: Fases del Sistema de Gestión de Seguridad de Datos Personales (SGSDP).
Tomada de: INAI, *Guía para implementar un sistema de gestión de seguridad de datos personales. Taller Medidas de Seguridad*, [en línea] México, INAI, 2019, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://inicio.inai.org.mx/CalendarioCapacitacion/Taller%20SGDPMiriam%20Padilla.pdf*, p. 122.

4.1.3 Responsables de Protección de Datos Personales en Posesión de Sujetos Obligados

El título séptimo de la Ley General, abarca a los principales responsables en materia de protección de datos personales en posesión de sujetos obligados, siendo de manera semejante a la de transparencia, en los casos del Comité de Transparencia y la Unidad de Transparencia.

Las funciones sustantivas de estas áreas con las siguientes:

Unidad de Transparencia	Comité de Transparencia
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	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

Unidad de Transparencia	Comité de Transparencia
de datos personales.	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.

Como se puede apreciar, estas autoridades llevan a cabo funciones distintas pero complementarias. De hecho, la principal obligación de estas áreas es facilitar el ejercicio de los derechos ARCO, garantizar un adecuado tratamiento de los datos personales, como son el cumplimiento de los principios y deberes, la realización de transferencias, así como la contratación de prestadores de servicios que impliquen el tratamiento de los datos personales.[365]

4.1.4 De los Derechos ARCOP

El artículo 3°, fracción XI, define a los Derechos ARCO como los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales, mismo que consisten en:

[365] INAI, *Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Manual del Participante*, *op. cit.* p. 23.

Imagen: Derechos ARCO.
Tomada de: INFOCDMX, *Datos Personales y transparencia proactiva, COVID19,* [en línea] México, INFOCDMX, s.a, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://infocdmx.org.mx/covid19/proteccion/*

De acuerdo con la Ley General (Art. 52) los elementos y requisitos para ejercer los Derechos ARCO son los siguientes:[366]

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).

Imagen: Requisitos aplicables a la solicitud para el ejercicio de los derechos ARCO.
Tomada de: Recio Gayo, Miguel, *Capítulo II, Del ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición*, en Solange Maqueo, María, *Coord*. "Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Comentada" [en línea], México, INAI, 2018, [fecha de consulta: 4 de diciembre de 2022] Disponible en:

[366] Tomado de Recio Gayo, Miguel, *Capítulo II, Del ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición*, en Solange Maqueo, María, *op. cit*. p. 149.

https://transparencia.guanajuato.gob.mx/bibliotecadigital/normatividad/Ley_General_de_Proteccion_de_Datos_Personales_en_Posesion_de_Sujetos_Obligados_comentada.pdf p. 149.

En cuanto a los plazos pare el ejercicio de este derecho se pude tomar el siguiente cuadro.[367]

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.	
	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.	A partir del día siguiente a la recepción de la solicitud.
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.

Imagen: Relación de eventos y plazos previstos, que el responsable debe considerar para el ejercicio de derechos ARCO.

Tomada de: Recio Gayo, Miguel, *Capítulo II, Del ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición*, en Solange Maqueo, María, *Coord*. "Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Comentada" [en línea], México, INAI, 2018, [fecha de consulta: 4 de diciembre de 2022] Disponible en:
https://transparencia.guanajuato.gob.mx/bibliotecadigital/normatividad/Ley_General_de_Proteccion_de_Datos_Personales_en_Posesion_de_Sujetos_Obligados_comentada.pdf p. 150.

[367] *Ibidem*. p. 150.

Ahora bien, el ejercicio de los Derechos ARCO, tampoco son absolutos, lo anterior significa que existen causales de improcedencia al ejercicio de estos derechos, para lo cual la Ley General (Art. 55) dispone lo siguiente:[368]

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).

Imagen: Criterios y causales de improcedencia del ejercicio de los derechos ARCO.
Tomada de: Recio Gayo, Miguel, *Capítulo II, Del ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición*, en Solange Maqueo, María, *Coord*. "Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Comentada" [en línea], México, INAI, 2018, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://transparencia.guanajuato.gob.mx/bibliotecadigital/normatividad/Ley_General_de_Proteccion_de_Datos_Personales_en_Posesion_de_Sujetos_Obligados_comentada.pdf* p. 151.

[368] *Ibidem*. p. 151.

4.1.4.1 De la portabilidad de datos personales

Por lo que hace a la Portabilidad de Datos, la OCDE los define como “la capacidad (a veces descrita como un derecho) de una persona física o persona jurídica para solicitar que un titular de datos transfiera a la persona, o a un tercero específico, datos relativa a esa persona en un formato estructurado, de uso común y legible por máquina en un formato ad-hoc o de forma continua"[369]

La Ley Federal de Telecomunicaciones y Radiodifusión define la Portabilidad -LFT- (Art. 3, XLIV) como: “Derecho de los usuarios de conservar el mismo número telefónico al cambiarse de concesionario o prestador de servicio.”

La misma LFT dispone que las comercializadoras de servicios de telecomunicaciones deberán permitir la portabilidad numérica. (Art. 174, I)

Asimismo, son derechos de los usuarios, a la portabilidad del número telefónico dentro del plazo que determine el Instituto y la cual será gratuita. (art. 191, III) Los concesionarios no podrán cobrar al usuario final o abonado cargo alguno por la portabilidad de su número.

En lo que respecta al sector de telecomunicaciones el IFT no podrá imponer condiciones que inhiban la portabilidad del número telefónico, para lo cual, a solicitud del usuario, en caso de haberse comercializado otros bienes y servicios, estos deberán individualizarse y facturarse de forma independiente. (Art. 267, XIII)

Oscar Puccinelli comenta que 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.”[370]

> 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.[371]

[369] Organización para la Cooperación y el Desarrollo Económicos, , *Data portability, interoperability and digital platform competition,* [en línea], OECD, 2021, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://www.oecd.org/daf/competition/data-portability-interoperability-and-digital-platform-competition-2021.pdf* p. 10.
[370] Puccinelli, Oscar R. *Capítulo III. De la Portabilidad de los Datos*, en Solange Maqueo, María, *op. cit*. p. 157.
[371] *Ibidem*. p. 162.

La Ley General en su artículo 57 dispone que 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.

De lo anterior se entiende que la procedencia del derecho de portabilidad será:

1) Cuando el tratamiento se efectúe por medios automatizados o electrónicos y en un formato estructurado y comúnmente utilizado.
2) Los datos personales del titular se encuentren en posesión del sujeto obligado responsable o sus encargados.
3) Los datos personales conciernan al titular, o bien, a personas físicas vinculadas a un fallecido que tengan un interés jurídico.
4) El titular hubiere proporcionado directamente al responsable sus datos personales.
5) La portabilidad de los datos personales no afecte los derechos de terceros.

4.1.5 Recurso de Revisión

Se hace valer por el titular ante el organismo garante, y se tiene un plazo de 15 días para hacerse valer.

Procede en los siguientes supuestos:[372]

- Se clasifiquen indebidamente como confidenciales los datos personales.
- Se declare su inexistencia.
- Se declare la incompetencia por el responsable.
- Se entreguen datos personales incompletos.
- Se entreguen datos personales que no correspondan a lo solicitado.
- Se niegue el acceso, rectificación, cancelación u oposición de datos personales.
- No se dé respuesta al ejercicio de derechos ARCO en los plazos establecidos por la Ley.
- Se entreguen los datos personales en una modalidad o formato no solicitados o incomprensibles.

[372] Artículo 104 LGPDPPSO.

- Se inconforme el titular por los costos de reproducción, envío o tiempos de entrega.
- Se obstaculice el ejercicio de los derechos ARCO a pesar de ser procedente.
- No se dé trámite a una solicitud para el ejercicio de derechos ARCO.
- En los demás casos que dispongan las leyes.

Por lo que hace a los aspectos Procesales del recurso de revisión:

- Una vez admitido el recurso de revisión, el organismo garante podrá buscar una conciliación entre el titular y el responsable conforme al procedimiento previsto en la Ley.
- En caso de no alcanzarse una conciliación, el organismo garante:
- Tiene 40 días hábiles para resolver:
- Ampliación: 20 días hábiles más (por una sola ocasión).
- Tiene 5 días hábiles para prevenir al titular. La prevención ocurre cuando el escrito del recurso de revisión no cumple con los requisitos señalados y el organismo garante no cuenta con elementos para subsanarlos.
- Titular: 5 días hábiles para subsanar omisión.
- Tiene que aplicar la suplencia de la queja a favor del titular.

Esquemáticamente se tiene lo siguiente:[373]

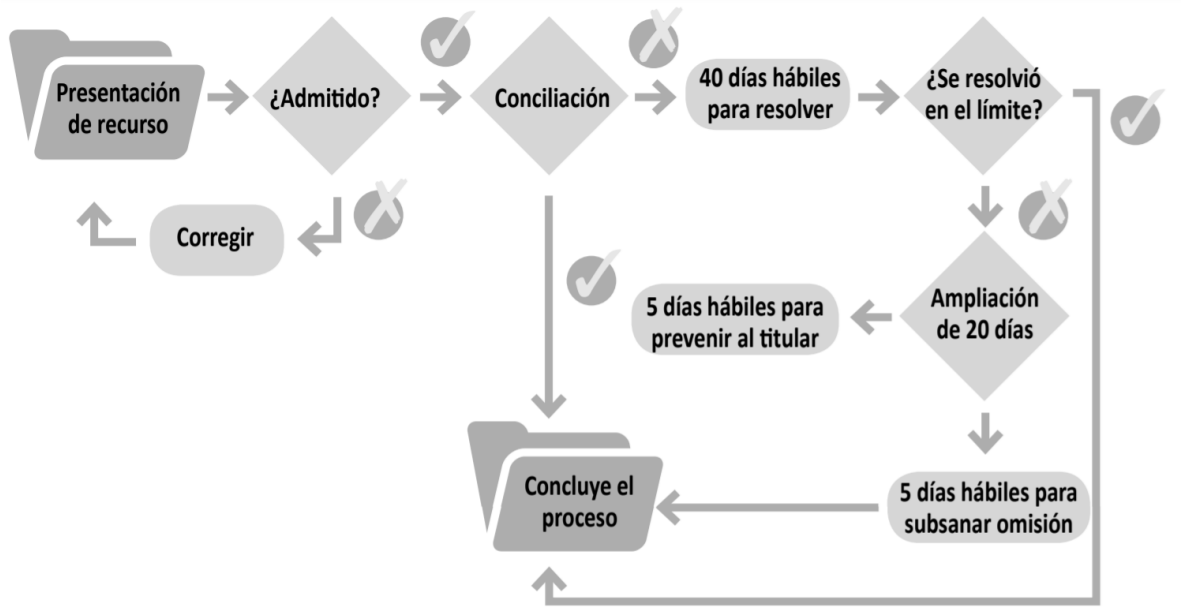


Imagen: Recurso de Revisión.
Tomada de: INAI, *Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Manual del Participante*, [en línea] México, INAI, 2017, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://cevinai-snt.inai.org.mx/repositorio/manuales/m_lgpdppso.pdf* p. 42.

[373] INAI, *Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Manual del Participante*, *op. cit*. p. 42.

4.1.6 Recurso de inconformidad

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.

El recurso de inconformidad procederá contra las resoluciones emitidas por los Organismos garantes de las Entidades Federativas que:[374]

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.

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 en que se hubiere notificado o se tenga conocimiento de la resolución dictada en la inconformidad.

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.

Las resoluciones del Instituto serán vinculantes, definitivas e inatacables para los

[374] Artículo 118 LGPDPPSO.

responsables y los Organismos garantes.

Los titulares podrán impugnar dichas resoluciones ante el Poder Judicial de la Federación mediante el juicio de amparo.

Finalmente, es importante señalar que, a diferencia de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, que tiene una aplicación en toda la República, en el caso de los sujetos obligados, cada entidad federativa tiene, a su vez su propia regulación.

En fin, la Protección de Datos Personales por parte de los sujetos obligados, apenas estamos dando los primeros pasos en la redefinición de su tratamiento, por lo que seguiremos observando su evolución e implementación.

4.2. En Posesión de Particulares

La protección de los datos personales o, en otras palabras, el derecho a la privacidad, es un derecho consagrado en las disposiciones internacionales de las cuales México es parte. En nuestro país, la Constitución protege a los particulares cuando se restringe la libertad de ideas y de imprenta cuando con ello se menoscabe a la persona; en este sentido, el concepto de privacidad y de datos personales ha evolucionado en el devenir del tiempo, y hoy más que nunca con el uso de las tecnologías de la información, se permite recabar, almacenar y transmitir información en tiempo real con fines diversos, lo que puede ocasionar serias amenazas a la privacidad como parte de intromisiones arbitrarias en la esfera privada de las personas.

En 2010, se publicó la Ley Federal de Protección de Datos Personales en Poder de los Particulares (LFPDPPP), cuya aplicación es en toda la República, y tiene por objeto la protección de los datos personales en posesión de los particulares con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

En cuanto a los sujetos regulados por esta ley, son las personas físicas o morales de carácter privado que realicen el tratamiento de datos personales. Este supuesto es amplio, pues desde que se hace la recopilación de cualquier dato personal, por parte de las Pymes o cualquier empresario en ejercicio de su función, está obligado a acatar las disposiciones normativas.

No obstante, se exceptúan de esta ley:[375]

- Las sociedades de información crediticia, como es el caso del Buró de Crédito.

[375] Artículo 2°, LFPDPPP.

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

El manejo de los datos personales es un punto sensible, por ello se debe entender que son datos personales cualquier información concerniente a una persona física identificada o identificable.

Asimismo, la ley incluye la definición de datos personales sensibles, considerando éstos como aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida dé origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.[376]

Cabe señalar que, en el caso de los sindicatos considerados como sujetos obligados en términos de la Ley General de Transparencia, el INAI ha comentado en diferentes foros que sí les es obligado publicar el padrón de sus afiliados sin que se considere violatorio de Datos Personales en Posesión de Particulares.

Asimismo, la LFPDPPP dispone como tratamiento de datos personales lo siguiente:[377]

[376] Artículo 3°, fracción VI, LFPDPPP.
[377] Artículo 3°, fracción XVIII, LFPDPPP.

Imagen: Tratamiento de Datos Personales.
Fuente: Elaboración propia

4.2.1 Principios de Datos Personales

El artículo 6° de la LFPDPPP dispone que Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, los cuales de manera esquemática son los siguientes:

Imagen: Tratamiento de Datos Personales.
Fuente: Elaboración propia

Por lo que hacen a los principios de finalidad lealtad, proporcionalidad y calidad; estos tienen un significado prácticamente igual que en el caso de protección de datos de sujetos obligados; por lo que se considera no repetir en este apartado. A continuación, se desarrollarán los otros principios en lo que hace a la parte propia de la LFPDPPP.

4.2.1 Principio de Licitud

Considero que, para lograr el debido y adecuado cumplimiento de este principio, se deben cumplir con más normas que para sujetos obligados.

El principio de licitud obliga al responsable a que el tratamiento sea con apego y cumplimiento a lo dispuesto por la legislación mexicana y el derecho internacional, a juicio del que esto escribe: la normatividad aplicable es la siguiente:[378]

<table>
<tr><td>Normatividad Obligatoria</td><td>Normatividad Complementaria</td></tr>
<tr><td>1. Ley Federal de Protección de Datos Personales en Posesión de Particulares
2. Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares
3. Lineamientos del Aviso de Privacidad</td><td>Legislación Nacional
▪ Ley General de Salud
▪ Ley General de los Derechos de Niñas, Niños y Adolescentes
▪ Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita
▪ Ley Federal de Protección al Consumidor
▪ Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares
▪ Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas

Internacional:
▪ Reglamento Europeo de Protección de Datos (GDPR)</td></tr>
<tr><td colspan="2">Normatividad INAI</td></tr>
<tr><td>Sistema de Gestión de Seguridad de Datos Personales

▪ Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales
▪ Guía para el Borrado Seguro de Datos Personales</td><td>Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales

▪ Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que</td></tr>
</table>

[378] Elaboración propia.

- Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas
- Manual en materia de seguridad basada en un entorno Microsoft® para MiPyMEs y organizaciones pequeñas mexicanas

Recomendaciones para el tratamiento de datos personales y cumplir con el deber de seguridad para Instituciones de Tecnología Financiera (ITF)

- Recomendaciones para el tratamiento de datos personales y cumplir con el deber de seguridad para Instituciones de Tecnología Financiera (ITF)

Tabla de equivalencia funcional entre estándares de seguridad y la LFPDPPP, su Reglamento y las Recomendaciones en materia de seguridad de datos personales

- Tabla de equivalencia funcional entre estándares de seguridad y la LFPDPPP, su Reglamento y las Recomendaciones en materia de seguridad de datos personales - Completa
- ISO/IEC 27001:2013
- ISO/IEC 27002:2013
- ISO/IEC 27005:2008
- ISO/IEC 27006:2011
- ISO/IEC TR 27008:2011
- ISO/IEC 29100:2011
- ISO/IEC 20000-1:2011
- ISO 22301:2012
- ISO 31000:2009
- ISO GUIDE 72
- ISO GUIDE 73
- ISO 9000:2005
- BS 10012:2009

impliquen el tratamiento de datos personales

Conformidad de contratos de adhesión de servicios de cómputo en la nube vs los criterios mínimos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales

- Conformidad de contratos de adhesión de servicios de cómputo en la nube vs los criterios mínimos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales

Guía de esquemas de autorregulación en materia de protección de datos personales

- Guía de esquemas de autorregulación en materia de protección de datos personales

Guía para la elaboración de evaluaciones de impacto a la privacidad

- Guía para la elaboración de evaluaciones de impacto a la privacidad

Recomendaciones para el manejo de incidentes de seguridad de datos personales

- Recomendaciones para el manejo de incidentes de seguridad de datos personales

Recomendaciones para reconocer las principales amenazas a los datos personales a partir de la valoración respecto al riesgo

▪ NIST SP 800-14 ▪ OECD Guidelines ▪ GAPP ▪ COBIT v4.1 ▪ COBIT 5 ▪ PCI DSS v2 ▪ HIPAA ▪ SOx ▪ ITIL v3 ▪ OWASP v2 ▪ CCM v3 *Metodología de Análisis de Riesgo BAA* ▪ Metodología de Análisis de Riesgo BAA *Toolkit de Concientización de Seguridad de Datos Personales para Responsables del Sector Privado* ▪ Toolkit de Concientización de Seguridad de Datos Personales para Responsables del Sector Privado	▪ Recomendaciones para reconocer las principales amenazas a los datos personales a partir de la valoración respecto al riesgo *Guía para el tratamiento de datos biométricos* ▪ Guía para el tratamiento de datos biométricos *Código de las buenas prácticas para orientar el tratamiento en línea de Datos Personales de niñas, niños y adolescentes* ▪ Código de las buenas prácticas para orientar el tratamiento en línea de Datos Personales de niñas, niños y adolescentes
Normas Mexicanas	
ables	Proyectos
NMX-I-319-NYCE-2018 NOLOGÍAS DE LA INFORMACIÓN-TÉCNICAS DE SEGURIDAD-ESCUELAS RESPONSABLES EN EL USO DEL INTERNET. (DOF: 11/09/2019) NMX-COE-001-SCFI-2018	PROY-NMX-I-27701-NYCE-2020 TECNOLOGÍAS DE LA INFORMACIÓN-TÉCNICAS DE SEGURIDAD-EXTENSIÓN DE LA NMX-I-27001-NYCE-2015 Y LA NMX-I-27002-NYCE-2015 PARA LA GESTIÓN DE LA PRIVACIDAD DE LA INFORMACIÓN-REQUISITOS Y LINEAMIENTOS PROY-NMX-I-22320-NYCE-2020 TECNOLOGÍAS DE LA

MERCIO ELECTRÓNICO – DISPOSICIONES A LAS QUE SE SUJETARÁN AQUELLAS PERSONAS QUE OFREZCAN, COMERCIALICEN O VENDAN BIENES, PRODUCTOS O SERVICIOS. (DOF: 30/04/2019) -I-1362-NYCE-2021 ECOMUNICACIONES-PROCEDIMIENTO SIMPLE DE ENCRIPTACIÓN PARA ENTORNOS DE INTERNET DE LAS COSAS (IOT) (DOF: 08/02/2022) -I-22301-NYCE-2021 NOLOGÍAS DE LA INFORMACIÓN-SEGURIDAD Y RESILIENCIA-SISTEMAS DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO-REQUERIMIENTOS (CANCELA A LA NMX-I-22301-NYCE-2015) [DOF: 08/02/2022] -I-22316-NYCE-2021 NOLOGÍAS DE LA INFORMACIÓN-SEGURIDAD Y RESILIENCIA-RESILIENCIA ORGANIZACIONAL-PRINCIPIOS Y ATRIBUTOS [DOF: 08/02/2022] -I-22320-NYCE-2021	INFORMACIÓN-SEGURIDAD Y RESILIENCIA-GESTIÓN DE EMERGENCIAS-DIRECTRICES PARA LA GESTIÓN DE INCIDENTES. PROY-NMX-I-22316-NYCE-2020 TECNOLOGÍAS DE LA INFORMACIÓN-SEGURIDAD Y RESILIENCIA-RESILIENCIA ORGANIZACIONAL-PRINCIPIOS Y ATRIBUTOS. PROY-NMX-I-22301-NYCE-2020 TECNOLOGÍAS DE LA INFORMACIÓN-SEGURIDAD Y RESILIENCIA-SISTEMAS DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO-REQUERIMIENTOS (CANCELARÁ A LA NMX-I-22301-NYCE-2015).

NOLOGÍAS DE LA INFORMACIÓN-SEGURIDAD Y RESILIENCIA-GESTIÓN DE EMERGENCIAS-DIRECTRICES PARA LA GESTIÓN DE INCIDENTES [DOF: 10/02/2022] -I-27018-NYCE-2021 NOLOGÍAS DE LA INFORMACIÓN-TÉCNICAS DE SEGURIDAD-CÓDIGO DE PRÁCTICA PARA LA PROTECCIÓN DE DATOS PERSONALES (DP) EN NUBES PÚBLICAS QUE ACTÚAN COMO ENCARGADOS DE DP (CANCELA A LA NMX-I-27018-NYCE-2016) [DOF: 10/02/2022]	

4.2.2 Principio de Consentimiento

De acuerdo con el artículo 3°, fracción IV de la LFPDPPP, el consentimiento es la manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos.

De manera esquemática el consentimiento se realiza de la siguiente manera:

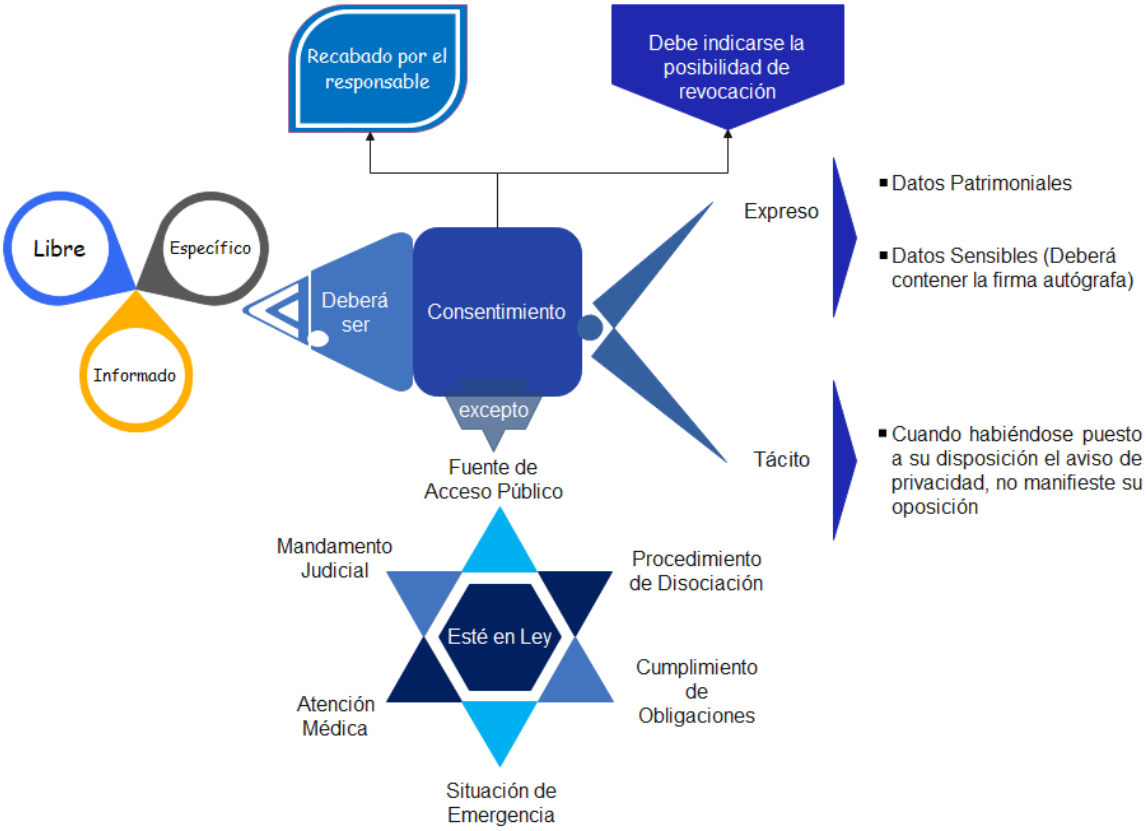


Imagen: Principio de Consentimiento.
Fuente: Elaboración propia

A continuación, anexo un consentimiento elaborado por un servidor:

[redacted]

[redacted] (En adelante [redacted]S) con domicilio en [redacted]; Código Postal 0[redacted], con página web ww[redacted]com, y con correo electrónico i[redacted].com es el responsable del tratamiento de sus datos personales, misma que será tratada en forma confidencial.

Esta declaración tiene por objeto informarle de sus derechos y obligaciones (Derecho de información en la recogida de datos), y las obligaciones que tiene L[redacted]S en la protección de datos personales recabados de Usted.

La obtención del presente consentimiento se elabora con base en la Ley Federal de Protección de Datos Personales en Posesión de Particulares (Arts. 8 y 9) del Reglamento de la Ley (Arts. 11 a 20), y los Lineamientos del Aviso de Privacidad.

El (la) que suscribe, **OTORGO MI CONSENTIMIENTO EXPRESO** a efecto de que L[redacted]S, recabe, proteja y trate los tipos de datos personales contemplados en el Aviso de Privacidad Integral de [redacted]S:

1) Datos de identidad y contacto
2) Datos Patrimoniales y Financieros
3) Datos Sensibles
4) Datos Laborales

Asimismo, autorizo expresamente el tratamiento de los Datos Personales, para las finalidades primarias y secundarias que se mencionan en el Aviso de Privacidad Integral de [redacted]S.

De igual forma, por lo que hace a la Transferencia de Datos otorgó expresamente el consentimiento para las transferencias y fines de las transferencias mencionadas en el Aviso de Privacidad Integral consistentes en:

Consentimiento
Tratamiento de Datos Personales

[redacted]

1. Bancos/Entidades Financieras
2. Sistema de Administración Tributaria (SAT)
3. Autoridades Administrativas
4. Fedatarios Públicos
5. Aliados estratégicos o agentes comerciales de [redacted]
6. Broker Hipotecario

Para tales efectos, manifiesto que tengo pleno conocimiento del contenido del Aviso de Privacidad Integral relativo al tratamiento de mis datos personales, el cual también es público y consultable a través de la página de internet **www.[redacted]m**, y que me encuentro plenamente informado del nombre, domicilio y teléfono del Responsable del tratamiento de mis datos personales; del fundamento legal que lo faculta para llevarlo a cabo; de los datos personales que serán recabados, según sea el caso; de la finalidad de su tratamiento; del ciclo de vida de los mismos; de los mecanismos, medios y procedimientos disponibles para ejercer mis derechos de Acceso, Rectificación, Cancelación y Oposición (derechos ARCO) así como de la revocación de mi consentimiento; y del domicilio del responsable del tratamiento de mis datos personales.

Consiento EXPRESAMENTE que los datos personales, patrimoniales y financieros; así como los datos sensibles sean tratados y transferidos conforme a los términos y condiciones del Aviso de Privacidad Integral, así como del presente documento.

FECHA:

NOMBRE COMPLETO:

_____

FIRMA: _____

4.2.3 Principio de Información

Se puede decir que todos los principios de la LFPDPPP, están intrínsecamente inmersos en el principio de información, el cual se materializa a través del aviso de privacidad. Este documento es la llave para indicar a las personas la manera en que la empresa responsable de los datos va a realizar el tratamiento de los datos.

Por medio del principio de información el responsable deberá dar a conocer al titular la información relativa a la existencia y características principales del tratamiento a que serán sometidos sus datos personales a través del aviso de privacidad.

Vale la pena recordar que la protección de datos personales no es un tema que pase de moda. Tanto sujetos obligados como particulares, están obligados a proteger, resguardar y cuidar los datos de las personas con las que tratan. En este sentido, la protección de datos personales forma parte del sistema de Transparencia, Acceso a la Información y Protección de Datos Personales, lo cual obliga a que tanto los Sujetos Obligados como particulares, cuenten con sus respectivos Avisos de Privacidad.

Cabe señalar que desde el 6 de julio de 2011 se venció el plazo para que las empresas generaran su aviso de privacidad; sin embargo, aun en 2022 existen diferentes particulares (personas físicas y morales) que, o no tienen avisos de privacidad o tener avisos de privacidad mal elaborados.

Hay que recordar que la LFPDPPP exige que, a partir de julio de 2011, todos los particulares que traten datos personales de particulares pongan a su disposición el aviso de privacidad, así como designar a la persona o en su caso, un departamento de datos personales que dará curso a las solicitudes de derechos ARCO, iniciadas por los titulares de los datos, la cual podrá encargarse también de la capacitación interna para permear las políticas y códigos de ética adoptados por la empresa, a efecto de proteger los datos personales que se tratan.

El aviso de privacidad, de acuerdo con el artículo 15 de la LFPDPPP, es un documento físico, electrónico o en cualquier otro formato generado por el responsable de datos personales, que es puesto a disposición del titular, previo al tratamiento de sus datos personales. El aviso de privacidad deberá contener, **al menos**, la siguiente información:

- Identidad y domicilio del responsable que los recaba.
- Finalidades del tratamiento de datos.
- Opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de datos.
- Medios para ejercer los derechos de acceso, rectificación, cancelación u oposición.
- Transferencias de datos que se efectúen.
- Procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad.

En el caso de datos personales sensibles, el aviso de privacidad deberá señalar expresamente que se trata de este tipo de datos.

Realmente existen diferentes tipos de categorías de datos personales además de los patrimoniales y sensibles a que hace referencia la LFPDPPP, de manera visual se coloca el siguiente cuadro:

Imagen: Categorías de datos personales.
Fuente: Elaboración propia

Además de los datos de personas morales equiparados a datos personales de los cuales ya se habló al inicio de este capítulo.

Cabe destacar que el hecho de que la propia ley manifieste el término “al menos” es un término que debe tomarse con mucho cuidado, toda vez que dependiendo el

tipo de actividades del responsable, podrían darse otro tipo de requisitos, como el caso del manejo de redes sociales, cookies; etc.

Asimismo, las características básicas del aviso de privacidad las podemos ver en el siguiente cuadro:

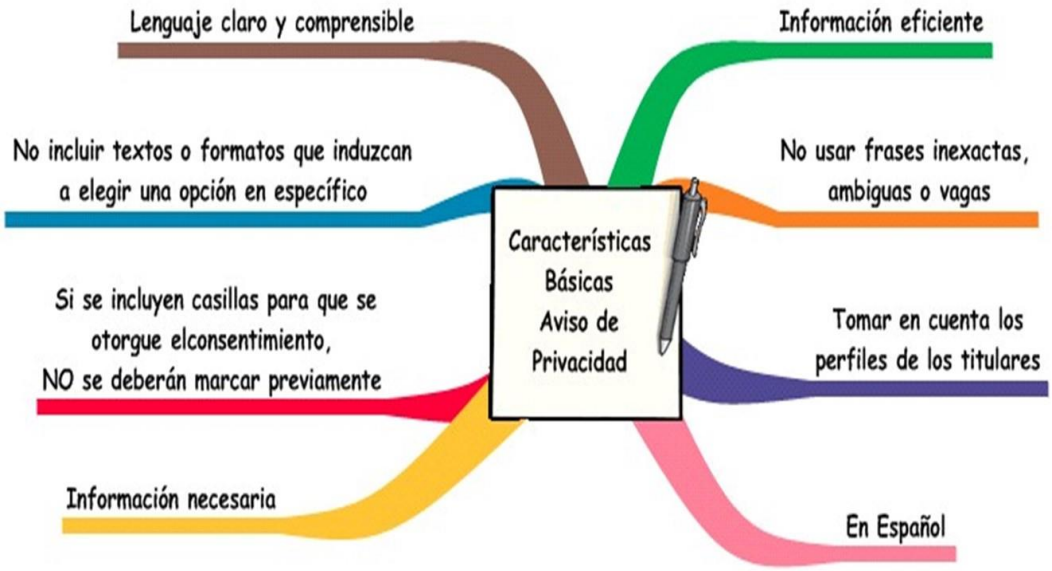


Imagen: Características del Aviso de Privacidad.
Fuente: Elaboración propia

El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología, de la siguiente manera:

- Cuando los datos personales hayan sido obtenidos personalmente del titular, el aviso de privacidad deberá ser facilitado en el momento en que se recaba el dato de forma clara y fehaciente, a través de los formatos por los que se recaban, salvo que se hubiera facilitado el aviso con anterioridad.
- Cuando los datos personales sean obtenidos directamente del titular por cualquier medio electrónico, óptico, sonoro, visual, o a través de cualquier otra tecnología, el responsable deberá proporcionar al titular, de manera inmediata, al menos la información correspondiente a la identidad y domicilio del responsable que los recaba, las finalidades del tratamiento de datos, así como proveer los mecanismos para que el titular conozca el texto completo del aviso de privacidad.

Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá dar a conocer el cambio en el aviso de privacidad, es decir, que las empresas deberán contar con dos tipos de avisos de privacidad: completo y simplificado también conocido como *short notice*.

Es importante señalar que el *short notice* no es otro aviso de privacidad, sino una especie de resumen del aviso completo, lo cual se genera como una forma de

simplificar el conocimiento al particular de la finalidad del tratamiento de sus datos personales. Además, el hecho de tener el *short notice* no obsta para que se deje de contar con el aviso completo, por lo que, en este caso, el responsable deberá comunicar en el mismo *short notice*, dónde se encuentra el aviso completo para su consulta.

Esto resulta práctico, si se toma en consideración que muchos dispositivos portátiles como tabletas o los *smartphones* tienen acceso a la red, y que este tipo de avisos facilitaría la lectura en cualquiera de estos dispositivos o cualquier otro análogo. Por lo que respecta a la elaboración de los avisos de privacidad, tanto la Secretaría de Economía (SE) como el INAI emitieron una guía para generar el aviso de privacidad donde, entre otros temas, emiten una serie de recomendaciones para la elaboración del aviso de privacidad:[379]

1) Conozca sus obligaciones y deberes.
2) Identifique actividades y/o procedimientos en los que utiliza datos personales.
3) Identifique el flujo de la información.
4) Identifique cómo obtiene los datos personales.
5) Identifique para qué fines utiliza los datos personales y qué tipo de datos trata.
6) Identifique las transferencias de datos personales que realice.
7) Identifique el perfil de los titulares de los datos personales.
8) Identifique los mecanismos que ofrece para que los titulares decidan sobre sus datos personales.
9) Piense en la información que hable sobre usted.

Con estas recomendaciones, las autoridades buscan que los particulares que detenten datos personales conozcan lo siguiente:[380]

- Los principios y deberes que rigen la protección de los datos personales.
- Identificar las actividades que requieran de un aviso de privacidad.
- En qué parte de la actividad y/o procedimiento se recaban los datos.
- Qué departamentos o personas tratan los datos y para qué funciones.
- Si se requiere una transferencia de datos, cuáles son sus finalidades y cómo las van a regular.
- El tiempo de conservación de datos y medios de su eliminación.
- Definir el momento en que se debe poner a disposición del particular

De manera similar a los sujetos obligados, el INAI diseñó la herramienta del Generador de Avisos de Privacidad (GAP), el cual tiene como finalidad apoyar a los particulares en la elaboración de su aviso de privacidad. Me gustaría comentar que cuando utilicé esta herramienta, me llamó la atención que, al ingresar, aparece la

[379] INAI, *Guía práctica para generar el aviso de privacidad*, [en línea], México, IFAI(INAI), 2011, [fecha de consulta: 4 de agosto de 2021], *http://www.itei.org.mx/v3/micrositios/privacidad/documentos/privacidadguia.pdf* p. i.
[380] Basado en *ibidem*. pp. 15-18.

leyenda que es responsabilidad del usuario el empleo de esta herramienta; por lo cual considero que esta herramienta tiene poco valor para responsables que realicen un tratamiento complejo de datos personales.

Actualmente muchos responsables tienen por hábito de calidad, el que al final de la prestación del servicio piden que se les proporcione un comentario o sugerencia, o aplican una encuesta de satisfacción, o simplemente piden los datos de los clientes a fin de mantener contacto con los clientes respecto de las promociones del lugar. Ahora necesitarán contar con la autorización de los particulares para tratar o usar los datos personales, de manera responsable.

Independientemente de lo anterior, los consumidores disponen de otra herramienta en caso de que no quieran ser "molestados" con propaganda vía telefónica por parte de las empresas. Sobre el particular, la Procuraduría Federal de Protección al Consumidor ha venido implementado diferentes estrategias tendentes a este fin, al respecto actualmente se cuenta con el servicio del Registro Público de Consumidores (RPC, https://rpc.profeco.gob.mx/) por medio del cual los particulares pueden solicitar que las empresas no envíen comunicación.

De manera general, las autoridades han recomendado algunas formas para elaborar el aviso de privacidad. Sin embargo, es necesario precisar que dependerá de las necesidades de cada empresa el ampliar o no el fin del aviso de privacidad, de hecho, se debe tratar con sumo cuidado la redacción en cuanto a los fines que persigue el aviso, a efecto de que se cubran todos los puntos correspondientes.

Adicionalmente, se tiene que tomar en consideración el Reglamento de la Ley y los Lineamientos del Aviso de Privacidad, así como otro tipo de leyes según la actividad a la que se dedique la empresa, se tienen que ver leyes en materia de prevención de lavado de dinero, laboral, protección a los niños y adolescentes, telecomunicaciones, derechos de autor, derecho a la imagen, etcétera; lo que hace que el Aviso de Privacidad sea un documento complejo.

Por lo anterior, a continuación, se presenta un cuadro con los errores más frecuentes al elaborar un Aviso de Privacidad, así como una breve recomendación de cómo atenderlos:[381]

ERRORES MÁS FRECUENTES	FORMA DE ATENDERLOS
1) Copiar el Aviso de Privacidad Integral de diferentes fuentes.	Se recomienda hacer un Aviso Acorde a la actividad de la PYME y su complejidad normativa

[381] Torres Jiménez Raúl, *Errores y horrores en la elaboración e implementación del aviso de privacidad*, [en línea], México, Revista consultoría, julio 18, 2017, [fecha de consulta: 4 de diciembre de 2022] *https://revistaconsultoria.com.mx/errores-y-horrores-en-la-elaboracion-e-implementacion-del-aviso-de-privacidad-parte-2/*

ERRORES MÁS FRECUENTES	FORMA DE ATENDERLOS
2) Falta de Identificación de los Datos y Tipos de Datos	Se recomienda se para los datos indicando expresamente cuáles son Datos Sensibles, y los de carácter patrimonial. Asimismo, se deben tener debidamente identificadas las categorías de datos: Identificación y Contacto, de Trabajadores, de Menores de Edad, etc.
3) Formas de otorgar y revocar el Consentimiento	Se recomienda elaborar documentos con consentimientos para datos sensibles y patrimoniales, así como para trabajadores en su caso. De igual forma se necesita mencionar en el Aviso de Privacidad la forma en la que se "retira" el consentimiento.
4) Falta de Cuidado de los datos personales al interior de la organización	Dentro de la Empresa, es necesario tener medidas técnicas y administrativas en el cuidado de los Datos Personales
5) Falta de diferenciación en las finalidades del tratamiento de los datos	Se recomienda separar los fines principales de los secundarios
6) Falta de elaboración de modalidades del Aviso de Privacidad	Se deben tener los Avisos integral, simplificado y corto; además de analizar si por el tipo de actividad se pueden contar con otros tipos de Aviso, como en caso de Videovigilancia.
7) Falta de identificación de transferencia y/o remisión de datos personales	Hay que indicar con quienes se comparte la información, ya sea autoridad, otros particulares u otras empresas del mismo grupo.
8) Falta de identificar las leyes relacionadas con la actividad	Saber si es una empresa de Salud, de Seguros, si son Sindicatos, empresas para niños, Asociaciones Civiles, de Telecomunicaciones, franquicias, del Sector Crediticio, etc., con el fin de tener claridad sobre que otras leyes se deben considerar al momento de elaborar el Aviso.
9) Falta de identificación de responsabilidades por manejo de aplicaciones (app) para celulares	Colocar en la app., los permisos que se necesitan para descargarla solicitando solo los estrictamente indispensables. El INAI ha establecido "sincronizar aplicaciones (app's) con redes sociales

ERRORES MÁS FRECUENTES	FORMA DE ATENDERLOS
	pudiera resultar riesgoso para la protección de datos personales, ya que el intercambio de información puede llegar a países donde no existen leyes que vigilen este derecho humano"[382]
10) Falta de Identificación para designar el responsable de los datos al interior de la organización y el procedimiento de acceso de derechos Arco	Hay que tener un nombre de persona física que sea la responsable al interior de la organización, de atender las solicitudes de Derechos ARCO. Asimismo, se deberá indicar el procedimiento con los datos tanto de identificación como de plazos de respuesta.
11) En caso de Avisos de Privacidad en Internet, tener marcadas "por default" las casillas de "acepto"	Evitar tener marcadas casillas de aceptación u otro tipo de leyendas al momento de colocar el Aviso de Privacidad o solicitar consentimientos.
12) No indicar el manejo de tecnologías de rastreo en la página web (cookies) y/o en el cuerpo de Aviso de Privacidad	Colocar al momento de abrir la página de internet que se utilizan tecnologías de rastreo o similares.
13) En caso de no tener página web, cómo dar a conocer que la empresa cuenta con Aviso de Privacidad	En todos los casos se deberá señalar la forma en la cual se dará a conocer el Aviso de Privacidad Integral.
14) Falta de indicaciones en el manejo de Redes Sociales	Generar contraseñas seguras. Configurar adecuadamente los niveles de seguridad. Procurar no hacer transacciones comerciales en redes sociales o en sitios web que se desprendan de éstas.[383]

Como se puede apreciar, el cuidado de los datos personales es un tema todavía novedoso, ya que será necesario revisar los avisos de privacidad y redactar los documentos adicionales o adecuaciones a documentos, toda vez que al interior de la organización de pueden establecer convenios de confidencialidad para el cuidado de los datos personales que se manejen; de igual forma la redacción de los consentimientos para el tratamiento de los datos según sean sensibles,

[382] INAI, *Boletín INAI/092/17*, México, INAI, 13 de abril de 2017, [fecha de consulta: 4 de agosto de 2021] Disponible en: *http://inicio.ifai.org.mx/Comunicados/Comunicado%20INAI-092-17.pdf*
[383] INAI, *Boletín INAI/089/17*, México, INAI, 10 de abril de 2017, [fecha de consulta: 4 de agosto de 2021] Disponible en: *http://inicio.ifai.org.mx/Comunicados/Comunicado%20INAI-089-17.pdf*

patrimoniales, laborales o de menores, formatos para ejercer adecuadamente los derechos ARCO.

Para terminar esta parte, se debe tomar en cuenta que se pueden varios avisos de privacidad, específicos según la actividad; por ejemplo, además del aviso de privacidad integral se pueden tener avisos para trabajadores, proveedores, maestros, entre otros, dependiendo siempre del tamaño y actividades que realicen.

4.2.4 Transferencia de Datos Personales

La transferencia implica la comunicación de datos personales dentro o fuera del territorio nacional, realizada a persona distinta del titular, del responsable o del encargado; en este sentido, cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento.

El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos.

Sobre las transferencias, el aviso de privacidad debe informar lo siguiente:

1) Si se realizan transferencias.
2) A quién se transfieren los datos personales, es decir, los terceros receptores o destinatarios de los datos personales. Puede hacerse de dos maneras:
    a. Identificando concretamente a cada uno por su nombre completo si se trata de una persona física, o por la denominación o razón social cuando sea una persona moral, o bien,
    b. Indicando el tipo o categoría de tercero receptor, por ejemplo, autoridades fiscales mexicanas, instituciones bancarias, agencias de viajes, aseguradoras, instituciones de asistencia social.
3) Para qué finalidades concretas se tratarán los datos transferidos.
4) Además, se debe identificar aquellas finalidades para las cuales se requiera el consentimiento del titular, por no encontrarse en los supuestos previstos en el artículo 37 de la Ley.[384]

Las condiciones de la transferencia de datos personales las podemos ver en el siguiente cuadro:

[384] INAI, *El ABC del Aviso de Privacidad*, [en línea], México, INAI, s.a., [fecha de consulta: 4 de diciembre de 2022] Disponible en: *http://abcavisosprivacidad.ifai.org.mx/#seccion3_06*

Imagen: Condiciones de transferencia de datos personales.
Fuente: Elaboración propia

Un ejemplo de cómo se puede redactar este contenido de información bajo el supuesto de que el responsable realiza transferencias nacionales e internacionales que requieren el consentimiento del titular es el siguiente:

¿Con quién compartimos su información y para qué fines?

Le informamos que sus datos personales son compartidos dentro y fuera del país con las siguientes personas, empresas, organizaciones y autoridades distintas a nosotros, para los siguientes fines:

Destinatario de los datos personales	Finalidad	País (Opcional)	Requiere Consentimiento
Secretaría de Salud del Distrito Federal	Para el cumplimiento de las obligaciones sanitarias que nos impone la Ley [...]	México	NO
Health Network	Para el ofrecimiento de los servicios que presta dicho centro, así como	San Francisco, California,	SI

	de promociones especiales. En su caso, para realizar los trámites de registro e inscripción, cuando usted decide tomar los cursos especializados que ofrece el centro.	EUA	

Adicionalmente, cuando se vayan a realizar transferencias de datos personales que requieran el consentimiento del titular, deberá incluir una cláusula que permita al titular indicar si acepta o no la transferencia de su información personal.

En su redacción, deberá tomar en cuenta el tipo de datos que va a transferir (patrimoniales, financieros, sensibles, u otro tipo), para que obtenga el consentimiento según corresponda: expreso, expreso y por escrito o tácito.
Ejemplo de cláusula para consentimiento tácito:

> ¿Con quién compartimos su información y para qué fines?
> [...]
> Le informamos que para las transferencias indicadas con un asterisco (*) requerimos obtener su consentimiento. Si usted no manifiesta su negativa para dichas transferencias, entenderemos que nos lo ha otorgado.
> No autorizo que mis datos personales sean compartidos con los siguientes terceros:
> [...]

Ejemplo de cláusula para consentimiento expreso:

> ¿Con quién compartimos su información y para qué fines?
> [...]
> Le informamos que para las transferencias indicadas con un asterisco (*) requerimos obtener su consentimiento expreso:
> Otorgo mi consentimiento para las siguientes transferencias de mis datos personales:
> [...]

Ejemplo de cláusula para consentimiento expreso y por escrito:
¿Con quién compartimos su información y para qué fines?
[...]
Le informamos que para las transferencias indicadas con un asterisco (*) requerimos obtener su consentimiento expreso y por escrito:

> Otorgo mi consentimiento para las siguientes transferencias de mis datos personales:
> [...]
>
> Nombre y firma del titular: _____

Adicionalmente, en este mundo donde cada vez los negocios rompen cada vez más y más fronteras, también los datos personales viajan a diferentes latitudes del orbe.

Por ello será necesario saber el tratamiento de los datos personales según el tipo de transferencia, tal como se aprecia en el siguiente cuadro:

Tipos de Transferencias	
Nacionales	**Extranjeras**
▪ La transferencia deberá formalizarse mediante algún mecanismo · Que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales	▪ El receptor deberá asumir las mismas responsabilidades que el Responsable ▪ Podrá valerse de cláusulas contractuales u otros instrumentos jurídicos · En los que se prevean al menos las mismas obligaciones a las que se encuentra sujeto el responsable que transfiere los datos personales, · Así como las condiciones en las que el titular consintió el tratamiento de sus datos personales

También hay que recordar que el Reglamento Europeo de Protección de Datos (RGPD) en su artículo 46 dispone lo siguiente:

Art. 46 Reglamento Europeo. Transferencias mediante Garantías Adecuadas

2. Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control por:

a) […]
b) normas corporativas vinculantes;
c) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión;
d) un código de conducta, o
e) un mecanismo de certificación.

De lo anterior entonces se puede advertir que:

1) Se deben señalar la transferencia y remisión de Datos
2) Se debe tener una tabla donde se indiquen a quién, con qué fines, y país de transferencia de datos personales
3) Se debe tener un consentimiento de datos personales en su caso

4.2.5 Principio de Responsabilidad

El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia o posesión, o por aquéllos que haya comunicado a un encargado, ya sea que este último se encuentre o no en territorio mexicano.

Para cumplir con esta obligación, el responsable podrá valerse de estándares, mejores prácticas internacionales, políticas corporativas, esquemas de autorregulación o cualquier otro mecanismo que determine adecuado para tales fines.

Por lo anterior, el responsable deberá adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.

Esquemáticamente el principio de responsabilidad abarca lo siguiente:

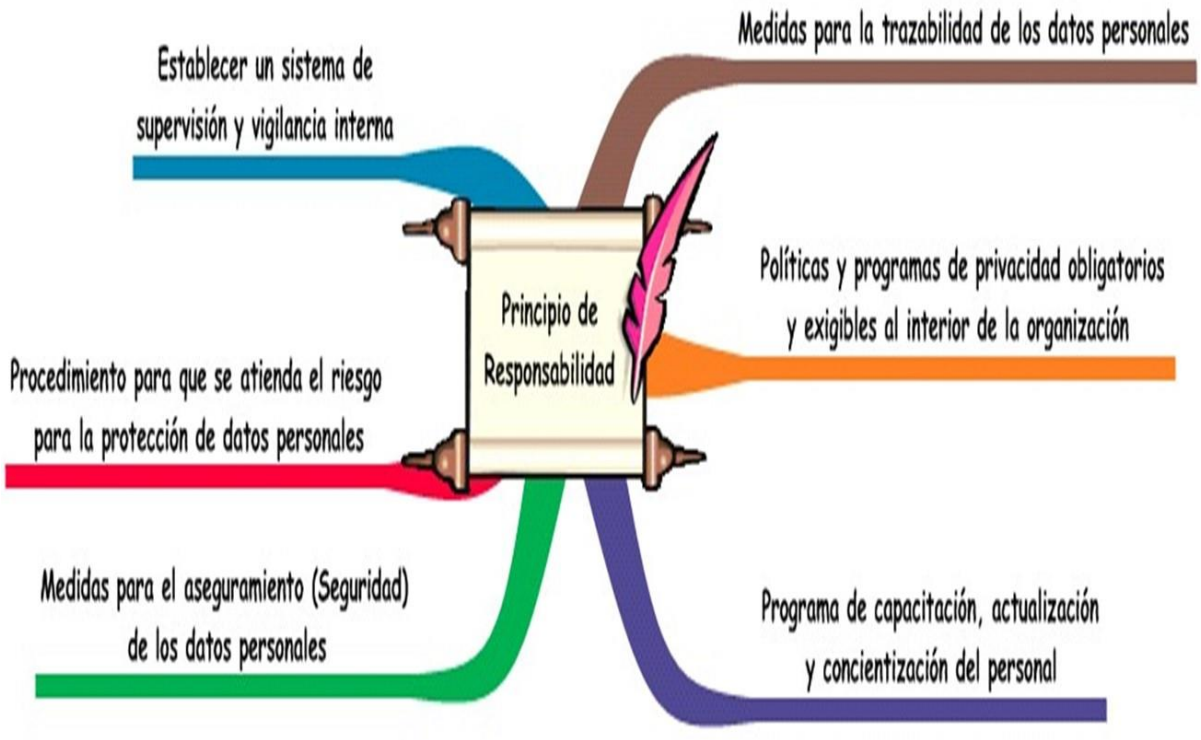


Imagen: Principio de responsabilidad.
Fuente: Elaboración propia

4.2.6 Cookies, Web Beacon y otras Tecnologías de Rastreo

De acuerdo con los Lineamientos del Aviso de Privacidad, por cookies y *web beacon* se entiende lo siguiente:

Cookies	Web Beacon
Archivo de datos que se almacena en el disco duro del equipo de cómputo o del dispositivo de comunicaciones electrónicas de un usuario al navegar en un sitio de internet específico, el cual permite intercambiar información de estado entre dicho sitio y el navegador del usuario. La información de estado puede revelar: ▪ medios de identificación de sesión, ▪ autenticación o ▪ preferencias del usuario, ▪ cualquier dato almacenado por el navegador respecto al sitio de internet.	Imagen visible u oculta insertada dentro de un sitio web o correo electrónico, que se utiliza para monitorear el comportamiento del usuario en estos medios. A través de éstos se puede obtener información como: ▪ Dirección IP de origen, ▪ navegador utilizado, ▪ sistema operativo, ▪ momento en que se accedió a la página.

Cuando el responsable utilice mecanismos en medios remotos o locales de comunicación electrónica, óptica u otra tecnología, que le permitan recabar datos personales de manera automática y simultánea al tiempo que el titular hace contacto con los mismos, en ese momento deberá informar al titular, a través de una comunicación o advertencia colocada en un lugar visible, sobre el uso de esas tecnologías y sobre el hecho de que a través de las mismas se obtienen datos personales, así como la forma en que se podrán deshabilitar, esto último salvo que dichas tecnologías sean necesarias por motivos técnicos.

A juicio del que esto escribe, todavía estamos en etapas muy incipientes respecto a la regulación de este tipo de tecnologías; no obstante, en Europa están más avanzados con motivos de su Reglamento de Protección de Datos Personales. En la Guía sobre el uso de las Cookies de la Agencia Española de Protección de Datos viene una clasificación más robusta de las categorías de cookies que existen, como se muestra a continuación:[385]

[385] Agencia Española de Protección de Datos, *Guía sobre el uso de las cookies*, España, AEPD , 2020, [fecha de consulta: 4 de diciembre de 2022] Disponible en: https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf pp. 11-13.

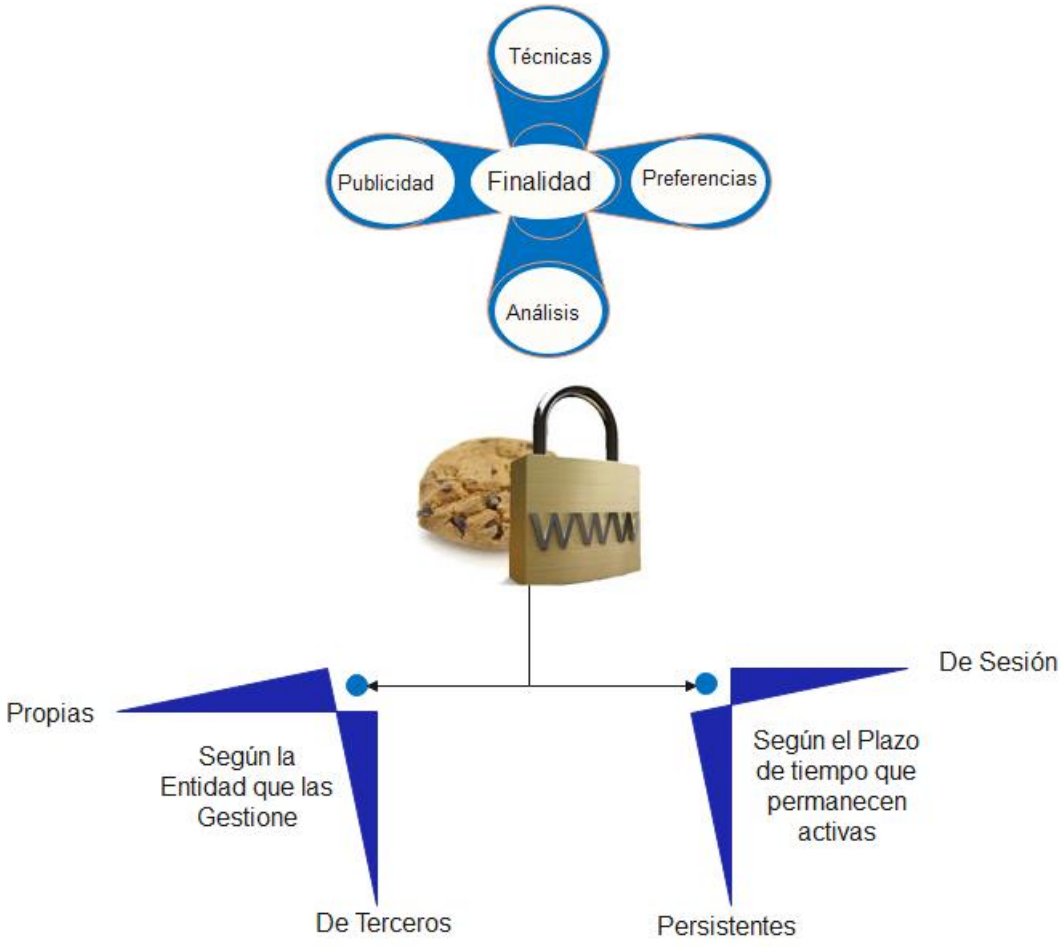


Imagen: Características de las cookies y otras tecnologías de rastreo.
Fuente: Elaboración propia

En la mencionada Guía, se publican diferentes ejemplos de anuncios de cookies dependiendo para que fin se utilicen y la forma de obtener el consentimiento por los datos que se obtienen.

Es de señalar que en caso de las denominadas *web beacon*, son en su naturaleza metadatos, de los cuales se hablará más adelante.

4.2.7 Medidas de Seguridad en la Protección de Datos Personales

Cuidar los datos personales fortalece también la credibilidad que se tiene con los clientes o beneficiarios, ya que tan solo en la Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales (ENAID) 2019[386], del Instituto Nacional de Estadística y Geografía (INEGI), reveló que a un 82.1% de la población que ha dado a conocer algún dato personal a alguna institución pública o empresa

[386] INEGI, *Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales 2019 (ENAID). Principales Resultados*, *op. cit.*

manifestó preocupación por el uso indebido de su número de cuenta o tarjeta del banco.

De la población que conoce o ha escuchado una Ley encargada de garantizar la protección de datos personales , 65.8% no recordó el nombre de esta, mientras que, 18,6% mencionó la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Esto representa un 10.2% de la población total que conoce la LFPDPPP.

Asimismo, 43.5% de la población manifestó que alguien se puso en contacto para ofrecer un servicio sin haber proporcionado sus datos personales durante 2019. Lo malo es que solo un 3.9% de la población presentó una queja por uso indebido de datos personales durante 2019.

El interés por la seguridad de los datos personales es por lo siguiente:

- La protección de datos personales es un derecho humano de los titulares de los mismos y una obligación para quienes los utilizan.
- Ayuda a prevenir y mitigar los efectos de una fuga y/o mal uso de los datos personales.
- Evita afectaciones económicas debido a multas, compensación de daños y pérdida de clientes e inversionistas.
- Aumenta la competitividad, mejora los procesos de la organización y el nivel de confianza de los consumidores, inversionistas y titulares.

Más allá de minimizar el posible impacto económico por la imposición de sanciones por parte de la autoridad, el principal beneficio de establecer medidas de seguridad, documentarlas y mantenerlas, radica en el aumento de la certidumbre y confianza de los titulares de los datos personales. Al mismo tiempo, se aumenta la competitividad del mercado en general, se mejoran los procesos de la organización y la eficiencia y se facilita la inversión.[387]

El Reglamento de la Ley en su artículo 47 establece como uno de los principios para la protección de datos personales, el de responsabilidad, que señala que toda persona física o moral que trate datos personales tiene la obligación de velar por su resguardo y uso adecuado.

Para ello, se debe comenzar por poner orden en los procesos y documentar los procedimientos. Algunas medidas para cumplir con este procedimiento, de acuerdo con el artículo 48 del Reglamento de la Ley, son la elaboración de políticas y programas de privacidad, el análisis de los riesgos a la privacidad en nuevos productos, las revisiones periódicas, entre otros.

El mantenimiento de forma segura de los sistemas a través de los que se obtienen,

[387] INAI, *Manual en Materia de Seguridad de Datos Personales para MIPYMES y organizaciones pequeñas*, México, INAI, 2015, [fecha de consulta: 26 de marzo de 2020] Disponible en: *http://inicio.ifai.org.mx/DocumentosdeInteres/Manual_Seguridad_Mipymes(Julio2015).pdf* p. 6.

almacenan, procesan y/o comparten datos personales, puede ser una tarea compleja, que requiere tiempo, recursos y conocimientos especializados. Sin embargo, esta tarea se facilita cuando quien trata datos personales identifica adecuadamente el uso de la información en cada uno de los procesos del organización o negocio, y este Manual le ayudará a esa tarea.

El cuidado de los datos personales es un tema todavía novedoso, y será necesario revisar los avisos de privacidad y redactar los documentos adicionales o adecuaciones a documentos, toda vez que al interior de la organización se pueden establecer convenios de confidencialidad para el cuidado de los datos personales que se manejen; de igual forma la redacción de los consentimientos para el tratamiento de los datos según sean sensibles, patrimoniales, laborales o de menores, formatos para ejercer adecuadamente los derechos ARCO, (Acceso, Rectificación, Cancelación, Oposición).

El Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas de junio de 2015 menciona diferentes amenazas típicas a la seguridad de los datos personales tal como se aprecia en el siguiente cuadro:

Imagen: Amenazas típicas a la seguridad de los datos personales.
Fuente: Elaboración propia. Tomado de: INAI, *Manual en Materia de Seguridad de Datos Personales para MIPYMES y organizaciones pequeñas*, México, INAI, 2015, [fecha de consulta: 26 de marzo de 2020] Disponible en: *http://inicio.ifai.org.mx/DocumentosdeInteres/Manual_Seguridad_Mipymes(Julio2015).pdf*

Como se puede apreciar, si bien desde 2015 ya existía un diagnóstico del tipo de sujetos son los que podrían poner en riesgo a las MIPYMES, lo cierto es que pocas hicieron algo tan solo por tener su aviso de privacidad, pero apenas se está viendo la luz en materia de seguridad al interior de las organizaciones derivado de la migración a operaciones digitales y comercio electrónico.

El Reglamento de la LFPDPPP en su artículo 61 establece las siguientes acciones para la seguridad de los datos personales:

1) Elaborar un inventario de datos y de sus medios de almacenamiento.
2) Determinar las funciones y obligaciones de las personas que traten datos personales.
3) Realizar un análisis de riesgos de los datos personales.
4) Revisar las medidas de seguridad existentes.
5) Realizar un análisis de brecha entre las medidas de seguridad existentes y las necesarias.
6) Elaborar un plan de trabajo para implementar las medidas de seguridad requeridas.
7) Realizar revisiones y auditorías del tratamiento de los datos y de las medidas de seguridad.
8) Mantener capacitado al personal relacionado con el tratamiento de los datos.

A través del Manual, los responsables y encargados de las micro, pequeñas y medianas empresas, así como de las organizaciones pequeñas, identificarán elementos de apoyo para cubrir cada una de estas acciones y así generar un esquema de seguridad continuo, consistente y efectivo.

Ahora bien, para el tratamiento de datos personales en tratándose de prestación de servicios, existen aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos, mediante condiciones o cláusulas generales de contratación, solo podrá utilizar aquellos servicios en los que el proveedor cumpla con los requisitos que se indican en el siguiente cuadro:[388]

Condiciones	**Mecanismos**
a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio d) Guardar confidencialidad respecto	a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido

[388] Elaborado a partir de INAI, *Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales*, [en línea] México, INAI, s.a., [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/ComputoEnLaNube.pdf* pp. 4-5.

de los datos personales sobre los que se preste el servicio	recuperarlos e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso

Por otra parte, el uso de las bases de datos apoya en los procesos de automatización de actividades dentro de los responsables, sin importar su tamaño, eficientando los procesos de comunicación, ventas y entrega; por ello, el uso de software de gestión empresarial resulta ser el complemento perfecto en las fases del proceso logístico.

No obstante, las bases de datos que manejen los responsables que ocupan la logística en sus procesos interactúan con datos personales, los cuales merecen una atención especial; por ello, resulta relevante el manejo e interacción con estos datos para las empresas.

La Ley Federal de Protección de Datos Personales en Posesión de Particulares define a las bases de datos como: "el conjunto ordenado de datos personales referentes a una persona identificada o identificable". En este sentido, la empresa responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.

Ahora bien, la gran pregunta está encaminada en la relación de las bases de datos con los programas de automatización que manejan las empresas que implementan en sus procesos logísticos toda vez que la empresa es la que será la responsable de establecer medidas técnicas y administrativas en el uso de las bases de datos; de hecho, en el reglamento de la ley en comento, se establece lo siguiente:

Medidas de seguridad técnicas. Conjunto de actividades, controles o mecanismos con resultado medible, que se valen de la tecnología para asegurar que:[389]

- El acceso a las bases de datos lógicas o a la información en formato lógico sea por usuarios identificados y autorizados;
- El acceso referido en el inciso anterior sea únicamente para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
- Se incluyan acciones para la adquisición, operación, desarrollo y mantenimiento de sistemas seguros, y
- Se lleve a cabo la gestión de comunicaciones y operaciones de los recursos informáticos que se utilicen en el tratamiento de datos personales.

Con base en lo anterior, las empresas que automatizan sus procesos logísticos deberán cuidar no solamente que los datos que ingresen en los sistemas sean verídicos y verificables, sino que además tendrán que cuidar la información a través de medidas adicionales, tomando en consideración que las empresas que realizan

[389] Artículo 2°, fracción VII, Reglamento de la LFPDPPP.

el licenciamiento de los sistemas de gestión logística o similares aún no cuentan con las medidas de seguridad que marcan las leyes de protección de datos en los diferentes países donde actúan.
En estos casos, la información personal con la que se vayan a manejar los clientes, proveedores, así como las distintas relaciones comerciales (en el manejo de las bases de datos), se sugiere lo siguiente:

1) Crear contraseñas seguras.
2) Controlar quiénes tienen acceso a las bases de datos.
3) Controlar quiénes pueden modificar las bases de datos.
4) Controlar el nivel de acceso que cada usuario tiene a las bases de datos.
5) Crear convenios de confidencialidad para proteger la información generada.
6) Informar en el aviso de privacidad de la creación de bases de datos, adicionando:
    a. El porqué es necesario crear y tener determinadas bases de datos.
    b. La remisión de información con la empresa gestora del software.
    c. Si es posible o no la cancelación de datos.
    d. De qué manera se pueden ejercer los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición).

De hecho, la LFPDPPP en su artículo 19 dispone que todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. De manera esquemática sería lo siguiente:

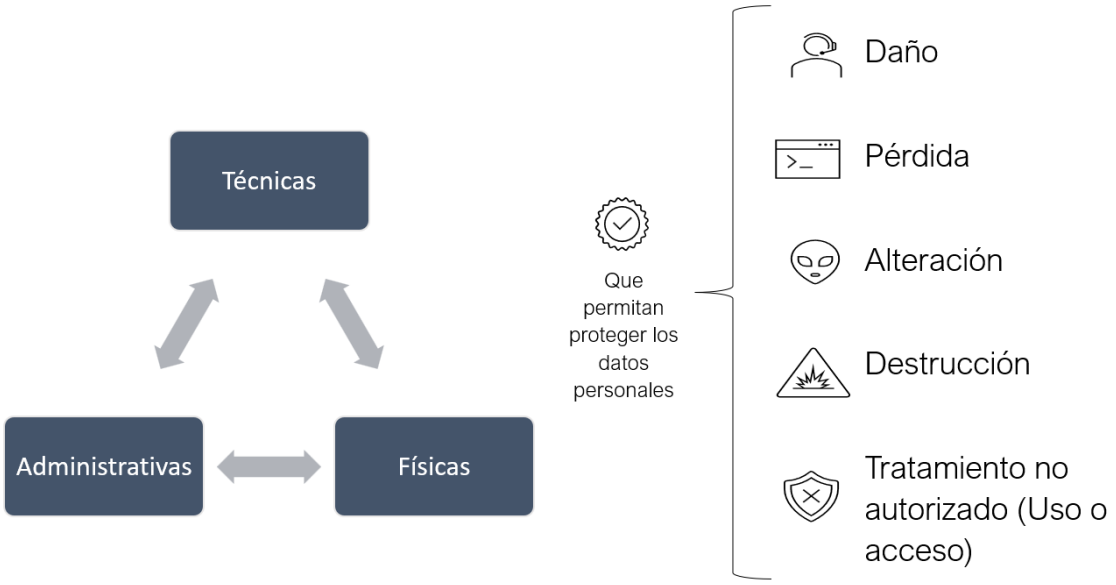


Imagen: Medidas de seguridad en los datos personales.
Fuente: Elaboración propia.

Ya en el reglamento de la LFPDPPP se establece en el artículo 2° en sus fracciones V, VI y VII en qué consisten dichas medidas, para lo cual nos puede servir el

siguiente esquema:

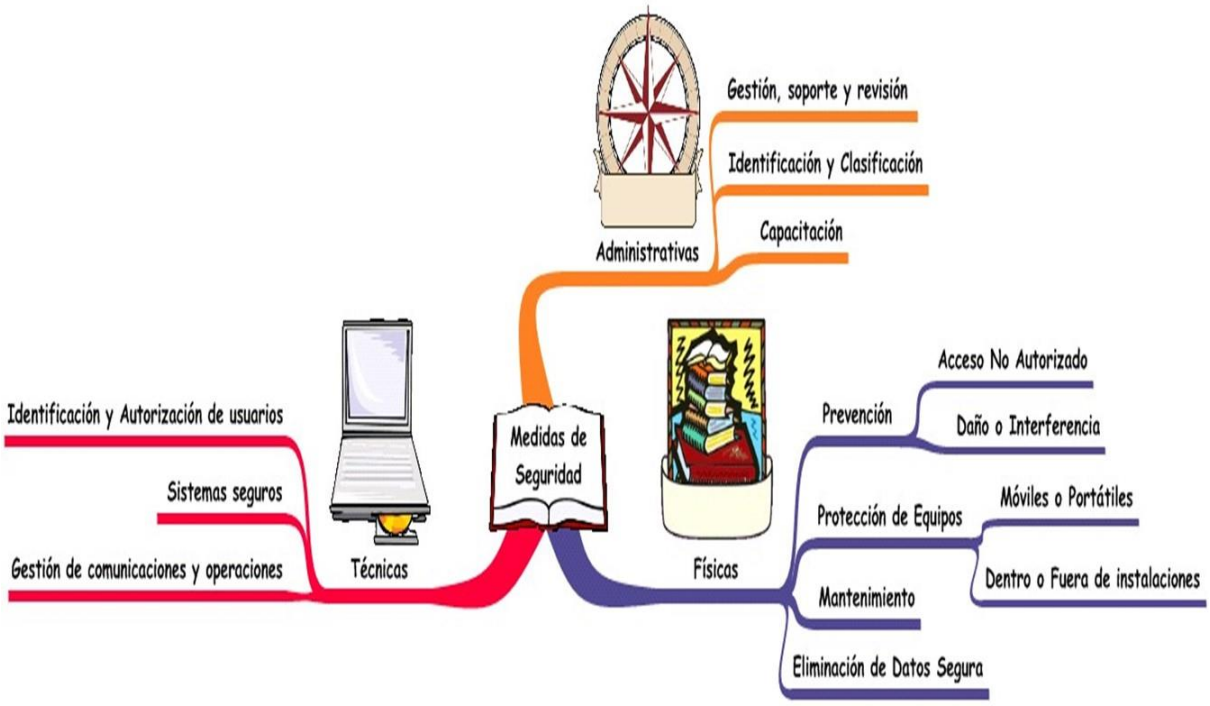


Imagen: Medidas de seguridad en los datos personales (ampliado).
Fuente: Elaboración propia.

Como se puede apreciar, el uso de las tecnologías de la información por medio de software en los procesos logísticos es cada vez más indispensable, pero también es igualmente necesario contar con medidas de protección adicionales, si no queremos que los clientes o proveedores se quejen ante la autoridad por no informarle que sus datos son almacenados en bases de datos y, peor aún, que no se les indique cómo hacer valer sus derechos.

4.2.8 Aspectos Informáticos de los Datos Personales (Datos en la Nube, Bases de Datos, Comercio electrónico, Metadatos)

El manejo de datos personales en el entorno digital es complejo y abarca los siguientes rubros:[390]

[390] Torres Jiménez, Raúl, *Implicaciones del manejo de datos personales en el entorno digital*, Revista Consultoría, núm. 51, México, julio 2016, p. 34.

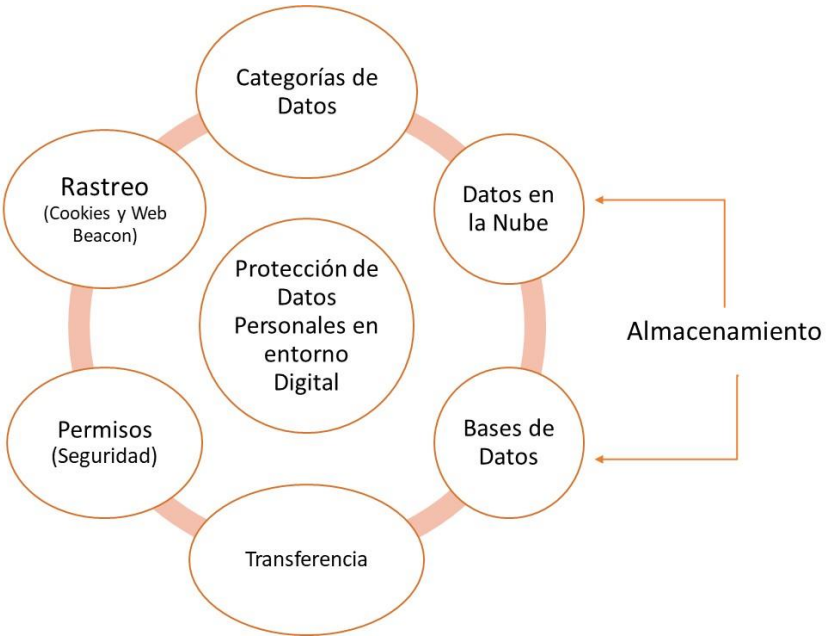


Imagen: Protección de Datos Personales en el entorno Digital.
Fuente: Elaboración propia. Tomado a partir de: Torres Jiménez, Raúl, *Implicaciones del manejo de datos personales en el entorno digital*, Revista Consultoría, México, núm. 51, julio 2016, p. 34.

Lo anterior, representa también una evolución en la forma de ampliar la migración del comercio (*e-commerce*) a los negocios electrónicos (*e-business*), cuyo término se emplea para "designar a empresas o negocios cuya actividad empresarial se basa fundamentalmente en la Red"[391]. De esta manera, más tarde que temprano las Pymes migrarán a una estructura de negocios electrónicos.

Es importante mencionar que entre más complejo sea el modelo de empresa o modelo de negocio, mayores aspectos son los que se tienen que cubrir; por ello es importante señalar algunas cuestiones de índole normativo tenemos que tomar en consideración si estamos empleando negocios electrónicos o estamos por migrar a este modelo:

1) Diseño de procesos del negocio con la ayuda de la tecnología: De tal manera que se aborden aspectos como digitalización del negocio, aplicaciones del negocio y demás integración del Internet de las Cosas considerando los aspectos de la Tecnología de la Información
2) Ciberseguridad: Manejos de los softwares como el antivirus, los cuales tienen módulos de seguridad de *malware, firewall*, protección de contraseñas, protección de datos personales entre otros. Cabe señalar que el pasado 26 de junio de 2018, se publicó en el Diario Oficial de la Federación (DOF) la Declaratoria de vigencia de la Norma Mexicana NMX-I-27032-NYCE-2018 misma que tiene que ver con Tecnologías de la información-Técnicas de seguridad-Lineamientos para la ciberseguridad.

[391] Asociación Mexicana de Internet, Estudio sobre Comercio Electrónico 2019, [Versión pdf] Disponible en https://www.asociaciondeinternet.mx/es/ p. 27.

3) Protección de la información de las bases de datos: Esta modalidad de la ciberseguridad tiene que ver con los sistemas CRM o ERP que manejen las empresas, por lo que deberán tener claros los términos y condiciones que manejen los proveedores de este tipo de servicios.
4) Condiciones de servicio de los proveedores de páginas web. Cuidar las medidas de seguridad HTTP"S", y otras medidas de salvaguarda.
5) Cuidar los contenidos: Sobre el particular es de hacer notar que los tribunales federales han indicado que las páginas web o electrónicas son hechos notorios y su contenido es susceptible de ser valorados en hechos judiciales.[392]
6) Manejo del marketing. El cual deberá contemplar cuidado con las promociones, imágenes, evitar publicidad engañosa, manejo de los contenidos en las diferentes redes sociales y demás canales de comunicación con los clientes.
7) Manejo de la Propiedad Intelectual. En este punto, las marcas, los avisos comerciales (slogans), la imagen comercial, denominaciones de origen, etc., son algunos de los derechos de propiedad industrial que se emplean al momento de dar a conocer los productos o servicios. No obstante, también son susceptibles de protegerse los sistemas de comercio electrónico; el sitio web, con derechos reservados, textos, música o videos. Incluso podrían crearse políticas relativas al desarrollo y protección de los materiales propiedad intelectual de la empresa.

De manera esquemática, el E-Commerce y los datos personales se vinculan de la siguiente manera:[393]

[392] PÁGINAS WEB O ELECTRÓNICAS. SU CONTENIDO ES UN HECHO NOTORIO Y SUSCEPTIBLE DE SER VALORADO EN UNA DECISIÓN JUDICIAL. Tesis: I.3o.C.35 K (10a.), Semanario Judicial de la Federación y su Gaceta, Décima Época, t. 2, noviembre de 2013, p. 1373.
[393] Torres Jiménez, Raúl, *Comercio Electrónico. Ventas seguras, amistades largas*, Revista Consultoría, México, edición especial junio 2021, *https://issuu.com/karimramos7/docs/edicion_especial_modificada* p. 29

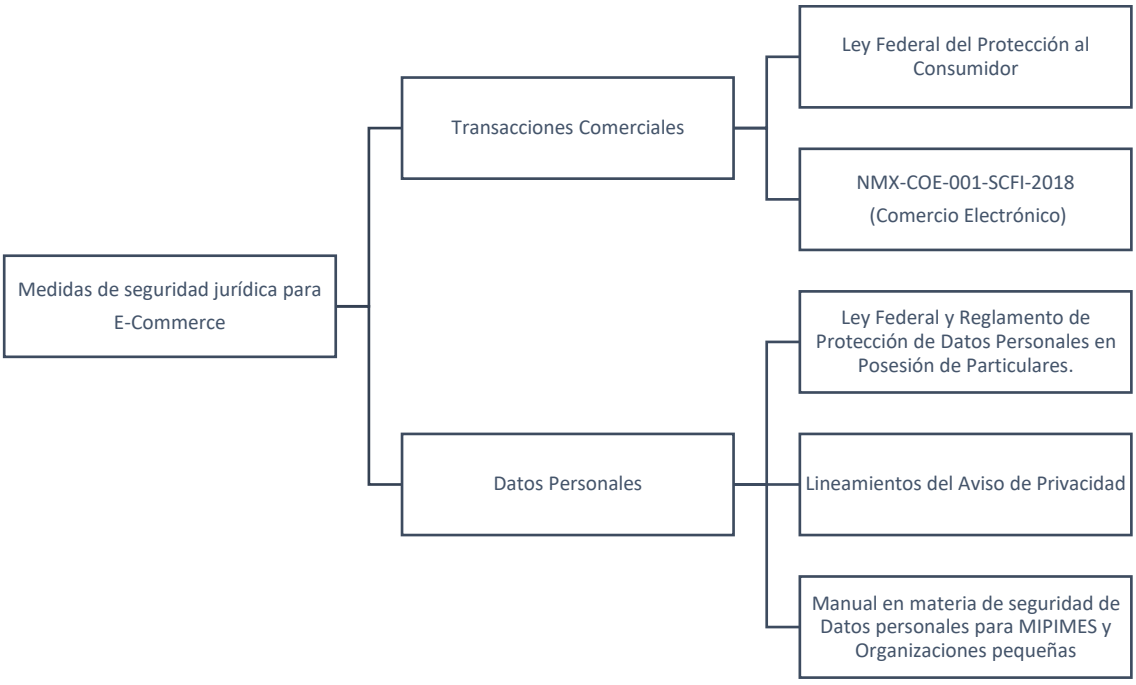


Imagen: Protección de Datos Personales en el entorno Digital.
Fuente: Elaboración propia.

Ahora bien, para el caso de tener simplemente la parte de comercio electrónico, además de existir infinidad de estrategias relacionadas con el tema, es importante destacar algunas obligaciones legales al momento de ejercer esta actividad. Por ello la Procuraduría Federal del Consumidor -Profeco- realiza periódicamente un monitoreo de tiendas virtuales[394], donde se revisan los siguientes puntos[395]:

[394] Profeco, *Monitoreo de Tiendas Virtuales*, [Versión HTML] Disponible en https://www.profeco.gob.mx/tiendasvirtuales/index.html
[395] Profeco, *Monitoreo de Tiendas Virtuales, ¿Qué revisamos a través del monitoreo de tiendas virtuales?*, [Versión HTML] Disponible en https://www.gob.mx/profeco/documentos/monitoreo-de-tiendas-virtuales-114564?state=published

Imagen: Monitoreo de Tiendas Virtuales de Profeco (puntos que se revisan).
Fuente: Elaboración propia.

Adicional a estos puntos, el pasado 30 de abril de 2019 se publicó en el DOF, la Declaratoria de vigencia de la Norma Mexicana NMX-COE-001-SCFI-2018, que tiene que ver con Comercio Electrónico – Disposiciones a las que se sujetarán aquellas personas que Ofrezcan, Comercialicen o Vendan Bienes, Productos o Servicios.

Esta Norma Mexicana establece las disposiciones a las que se sujetarán todas aquellas personas físicas o morales que en forma habitual o profesional ofrezcan, comercialicen o vendan bienes, productos o servicios, mediante el uso de medios electrónicos, ópticos o de cualquier otra tecnología, con la finalidad de garantizar los derechos de los consumidores que realicen transacciones a través de dichos medios, procurando un marco legal equitativo, que facilite la realización de transacciones comerciales, otorgando certeza y seguridad jurídica a las mismas.

De acuerdo con esta NMX, las transacciones comerciales en medios electrónicos, ópticos o de cualquier otra tecnología a través de un Sistema de información, deberán cumplir con:

1) Las especificaciones, características, condiciones y términos aplicables a los bienes, productos o servicios que se ofrecen:
    a. Información y Publicidad al Usuario o Consumidor.
    b. Términos y condiciones.
        i. Identificación del Proveedor.
        ii. Procedimiento para la adquisición del bien, producto o servicio.
        iii. Medios de Notificaciones o comunicación con el Consumidor.
        iv. Mecanismos de cambios o devoluciones.
        v. Mecanismos de solución de controversias:
        vi. Restricciones a menores de edad en su caso.
        vii. Condiciones de pago y facturación.
        viii. Mecanismos para aceptar términos y condiciones.
    c. Características aplicables a los bienes o productos o servicios.
    d. Mensajes publicitarios, perfil del Consumidor y comportamiento en línea.
2) Mecanismos para que el Consumidor pueda verificar que la operación refleja su intención de adquisición de los bienes, productos y servicios ofrecidos y las demás condiciones.
3) Mecanismos técnicos de seguridad para la aceptación, soporte de la prueba de la transacción y de identidad.
4) Mecanismos para garantizar la protección y confidencialidad de los datos personales del Usuario y del Consumidor.
5) Mecanismos de pago y de entrega.
6) Mecanismos para presentar dudas, reclamaciones o aclaraciones
7) Mecanismos para presentar cancelaciones, devoluciones o cambios de producto o servicios.

Por otra parte, existen otro tipo de datos que no son tan fáciles de identificar, son datos ocultos, pero que las empresas utilizan para saber más de nosotros; datos como: Historiales de consultas, segmentación de clientes, encabezados de archivos multimedia, catálogos de base de datos, etiquetas HTML de páginas web, direcciones IP, encabezados de emails, registros de llamadas telefónicas, etc.; estos datos de los datos son los llamados Metadatos, los cuales son datos descriptivos que versan sobre el concepto, calidad y condiciones o características de los datos.[396]

La Asamblea General de las Naciones Unidas en su acuerdo A/C.3/71/L.39 de fecha 31 de octubre de 2016, relativo al tema el derecho a la privacidad en la era digital, menciona que "si bien los metadatos pueden aportar beneficios, algunos tipos de metadatos, tomados en conjunto, pueden revelar información personal y pueden dar indicación del comportamiento, las relaciones sociales, las preferencias privadas y la identidad de una persona."[397]

La misma Asamblea General de las Naciones Unidas en su acuerdo A/HRC/23/40 de fecha 17 de abril de 2013 relacionado con el vigésimo tercer periodo de sesiones, relativo al Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, menciona que:

> El carácter dinámico de la tecnología no solo ha cambiado la forma en que puede llevarse a cabo la vigilancia, sino también "qué" puede vigilarse. Al facilitar la creación de oportunidades de comunicación e intercambio de información, Internet también ha posibilitado la elaboración de un gran volumen de datos de transacciones de personas y acerca de estas. Esta información, conocida como datos de las comunicaciones o metadatos, incluye información personal sobre particulares, su ubicación y actividades en línea, así como registros e información conexa sobre los correos electrónicos y los mensajes que envían o reciben.[398]

Por ello los metadatos circulan, en muchos casos, sin que responsable de Tratamiento de datos personales ni el Interesado lo sepan, por ello, datos de ubicación y fecha de una fotografía realizada por un teléfono móvil. De ahí que son tan valiosos para los algoritmos de búsqueda de empresas que manejan buscadores, redes sociales, CRM's, ERP's, Plantillas para elaboración de páginas web o empresas de telecomunicaciones (servicios de telefonía móvil)

---

[396] Torres Jiménez, Raúl, *Metadatos, el otro activo oculto de las empresas*, Revista Consultoría, México, diciembre de 2021, p. 46.

[397] Organización de las Naciones Unidas, *El derecho a la privacidad en la era digital*, [en línea] ONU, Acta A/C.3/71/L.39 de fecha 31 de octubre de 2016, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://www.acnur.org/fileadmin/Documentos/BDL/2017/10904.pdf* p. 3.

[398] Organización de las Naciones Unidas, *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión Frank La Rue*, [en línea] ONU, acuerdo A/HRC/23/40 de fecha 17 de abril de 2013, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/133/06/PDF/G1313306.pdf?OpenElement*p. 5.

El escándalo con WhatsApp de una supuesta transferencia de datos a Facebook que ocasionó que *Telegram* subiera de usuarios; no fue en realidad por la transferencia de Datos Personales sino por los metadatos asociados a los datos personales.

En el mundo de la gestión de bases de datos, los metadatos pueden abordar el tamaño y el formato u otras características de un elemento de datos; por ello, resulta fundamental interpretar el contenido de los datos de la base de datos.

"Los metadatos pueden ser datos personales y muchas veces lo son"[399], recuerda el director de la Agencia Española de Protección de Datos, José Luis Rodríguez. "Para que no sean datos personales tienen que ser anónimos, con una disociación irreversible", añade. Si, como en esta investigación, se puede hacer el camino inverso desde los metadatos a la identidad de la persona, entonces sí se le aplicaría la legislación sobre privacidad. Para Rodríguez, el problema de fondo es que "en la medida en que existe cada vez más información disponible, se debilita la anonimización porque hay más posibilidades de combinar y, por lo tanto, de identificar o individualizar a la persona".[400]

¿Qué tenemos en nuestro país? Muy poco. Tenemos tres normas principales: La Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP), El Reglamento de la Ley (RLFPDPPP) y los Lineamientos del Aviso de Privacidad (LAP). Adicionalmente se tienen diferentes documentos que ha emitido el INAI como buenas prácticas en el manejo de datos personales y otros medios de seguridad de los mismos.

En el RLFPDPPP tenemos una definición de qué es el entorno digital, “Es el ámbito conformado por la conjunción de hardware, software, redes, aplicaciones, servicios o cualquier otra tecnología de la sociedad de la información que permiten el intercambio o procesamiento informatizado o digitalizado de datos”[401]

Algunos de los metadatos están vinculados con las cookies. En este sentido, cuando el responsable utilice mecanismos en medios remotos o locales de comunicación electrónica, óptica u otra tecnología, que le permitan recabar datos personales de manera automática y simultánea al tiempo que el titular hace contacto con los mismos, en ese momento deberá informar al titular, a través de una comunicación o advertencia colocada en un lugar visible, sobre el uso de esas tecnologías y sobre el hecho de que a través de las mismas se obtienen datos personales, así como la forma en que se podrán deshabilitar, esto último salvo que dichas tecnologías sean necesarias por motivos técnicos. [402]

---

[399] Criado, Miguel Ángel, *Cuatro compras con la tarjeta bastan para identificar a cualquier persona*, [en línea] España, El País, Secc. Ciencia/Materia, 29 de enero de 2015, [fecha de consulta: 4 de diciembre de 2022] Disponible en:
https://elpais.com/elpais/2015/01/29/ciencia/1422520042_066660.html
[400] *Ídem.*
[401] Artículo 2°, fracción III, RLFPDPPP.
[402] Artículo Trigésimo primero de los Lineamientos del Aviso de Privacidad.

Europa, como siempre va más adelantado que nosotros, y en su Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas reconoce que "Del mismo modo, los metadatos derivados de las comunicaciones electrónicas también pueden develar información muy delicada y de carácter personal. Entre esos metadatos figuran los números a los que se ha llamado, los sitios web visitados, la localización geográfica o la hora, la fecha y la duración de una llamada, información que permite extraer conclusiones precisas sobre la vida privada de las personas participantes en la comunicación electrónica tales como sus relaciones sociales, sus costumbres y actividades de la vida cotidiana, sus intereses, sus preferencias, etc."

Por lo anterior, además del famoso aviso de privacidad, que solamente actúa como un cascarón de qué es lo que las empresas u otras organizaciones hacen con los datos personales; considero que lo conveniente es ir adoptando mecanismos de esquemas de autorregulación vinculante con el fin de que los responsables asuman medidas de seguridad técnicas, administrativas y físicas en e cuidado de los datos personales y, adicionalmente puedan acreditarse ante el INAI para poder usar el logotipo REA INAI.

4.2.9 Esquemas de Autorregulación Vinculante

La Autorregulación Vinculante es un conjunto de principios, normas y procedimientos, de adopción voluntaria y cumplimiento vinculante, que tiene como finalidad regular el comportamiento de los responsables y encargados respecto a los tratamientos de datos personales que lleven a cabo.

La regulación de estos esquemas la podemos ver en el siguiente esquema:

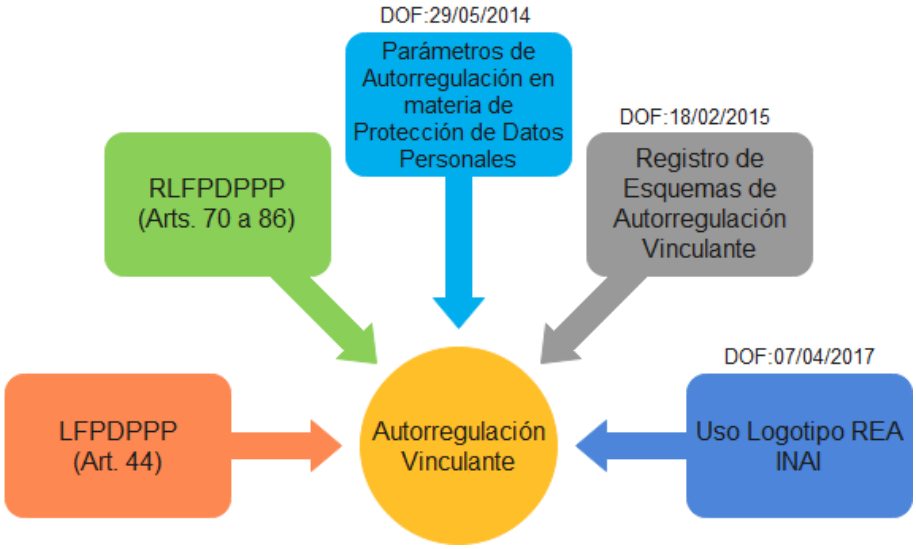


Imagen: Normatividad del esquema de autorregulación vinculante.
Fuente: Elaboración propia.

Adicionalmente, el INAI elaboró la Guía de Esquemas de Autorregulación con el fin de apoyar en la creación e implementación de los esquemas de autorregulación.[403]

La adhesión a los esquemas de autorregulación vinculante, por parte de un responsable o encargado es de carácter voluntario. No obstante, el cumplimiento de dichos esquemas será obligatorio para quienes se adhieran a los mismos, por lo que éstos deberán prever sanciones por su incumplimiento.

Los esquemas de autorregulación vinculante podrán incluir principios, normas y procedimientos para adecuar y armonizar las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, a la realidad de sectores específicos, y abordar problemáticas o situaciones particulares que no fueron previstas por la norma general, a fin de hacer eficiente la protección de datos personales en las actividades que se autorregulen.

Asimismo, la autorregulación vinculante permitirá elevar los estándares de protección de datos personales, a través de la adopción de las mejores prácticas en la materia, tanto nacionales como internacionales.

Estos esquemas autorregulatorios se basan en un sistema de gestión de datos personales o SGDP, el cual tiene como fin establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales en función del riesgo de los activos y de los principios, deberes y obligaciones previstos en la Ley, demás normativa aplicable y buenas prácticas en materia de protección de datos personales.

El SGDP deberá desarrollar las siguientes cuatro fases: planificar, hacer, verificar y actuar, de acuerdo con lo descrito en la tabla siguiente:[404]

	Elemento del SG	**Fase del ciclo PHVA**	**Actividades**
PROCESO	Metas	Planificar	Identificar políticas, objetivos, riesgos, planes, procesos y procedimientos necesarios para obtener el resultado esperado por el responsable o encargado (meta).
	Medios de acción	Hacer	Implementar y operar las políticas, objetivos, planes, procesos y procedimientos establecidos en la fase anterior.

[403] INAI, *Guía de Esquemas de Autorregulación en Materia de Protección de Datos Personales*, [en línea], México, INAI, 2016, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/GUIA%20AUTORREGULACION.pdf*

[404] Elaborado a partir de *Ibidem*. p. 19.

		Verificar	Evaluar y medir los resultados de lo implementado, a fin de verificar el adecuado funcionamiento del SGDP y el logro de la mejora esperada.
	Actuar	Adoptar medidas correctivas y preventivas en función de los resultados y de la revisión realizada, o de otra información relevante, para lograr la mejora continua.	

Un esquema de autorregulación vinculante debe contener los suguientes aspectos:[405]

Imagen: Autorregulación vinculante.
Tomado de: Padilla Espinosa Miriam, *Elementos de un esquema de autorregulación vinculante*, [en línea], México, TodoPDP, s.a. [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://todopdp.com/esquemas-de-autorregulacion/*

[405] Adaptado de Padilla Espinosa, Miriam, *Elementos de un Esquema de Autorregulación Vinculante*, TodoPDP, s/d, [Versión HTML] https://todopdp.com/esquemas-de-autorregulacion/

De acuerdo con la Guía de Autorregulación, el flujo para obtener este Registro de Esquemas de Autorregulación Vinculante (REA) es el siguiente:[406]

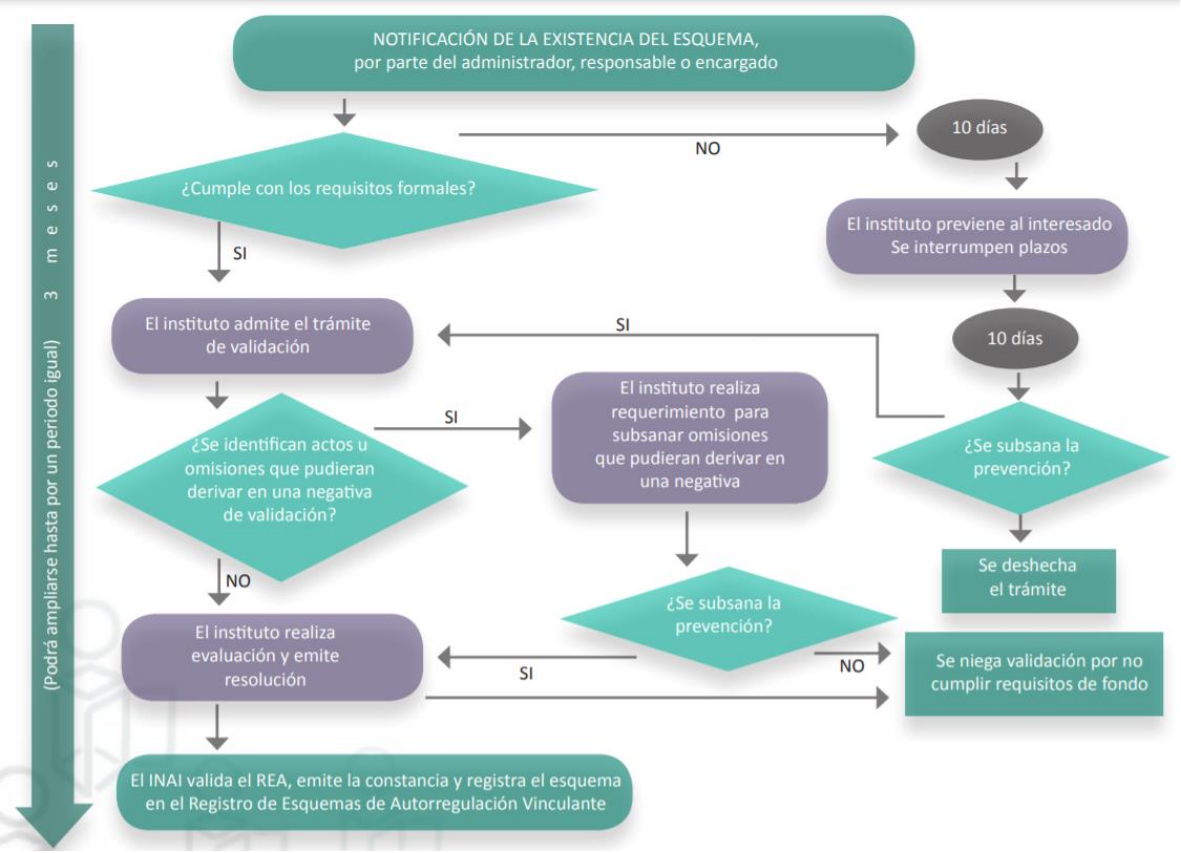


Imagen: Flujo del proceso de validación de autorregulación vinculante.
Tomado de: INAI, *Guía de Esquemas de Autorregulación en Materia de Protección de Datos Personales*, [en línea], México, INAI, 2016, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://home.inai.org.mx/wp-content/uploads/GUIA%20AUTORREGULACION.pdf* p. 33.

En caso de que la resolución del Instituto valide el esquema, se asignará un número único de registro. En este caso podrá hacer uso del logotipo "REA INAI" el cual podrá utilizarse exclusivamente para informar de manera gráfica que una entidad de acreditación, un organismo de certificación o un esquema de autorregulación vinculante se encuentran inscritos en el Registro, o bien, que un responsable o encargado está adherido o desarrolló un esquema de autorregulación vinculante inscrito en el REA.

[406] INAI, *Guía de Esquemas de Autorregulación en Materia de Protección de Datos Personales*, *op. cit*. p. 33.

4.2.10 Procedimientos en Materia de Protección de Datos Personales

4.2.10.1 *Procedimiento de Derechos ARCO*

Los titulares de los datos personales son las personas físicas que podrán ejercer por sí mismas o por medio de representante legal, los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO).

Es importante conocer cuáles son estos derechos que pueden hacer valer los titulares ante los responsables:[407]

- **Acceso**. Derecho del titular a e solicitar el acceso a sus datos personales que están en las bases de datos, sistemas, archivos, registros o expedientes del responsable que los posee, almacena o utiliza, así como de conocer información relacionada con el uso que se da a su información personal.
- **Rectificación**. Cuando los datos sean inexactos o incompletos, o no se encuentren actualizados.
- **Cancelación**. Derecho del titular que da lugar a que se eliminen (o supriman) de los archivos, registros, expedientes, sistemas, bases de datos del responsable que los posee, almacena o utiliza.
- **Oposición**. Derecho del titular a que no se utilicen para ciertos fines, o de requerir que se concluya el uso de los mismos a fin de evitar un daño a su persona.

El titular o su representante legal podrán solicitar al responsable en cualquier momento el acceso, rectificación, cancelación u oposición respecto de los datos personales que le conciernan. La solicitud deberá contener lo siguiente:[408]

- Nombre del titular y domicilio, u otro medio para comunicarle la respuesta a su solicitud.
- Los documentos que acrediten la identidad o, en su caso, la representación legal del titular.
- La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCO.
- Cualquier otro elemento o documento que facilite la localización de los datos personales.

El responsable comunicará al titular la determinación adoptada, a efecto de que, si resulta procedente, se haga efectiva. La obligación de acceso a la información se dará por cumplida cuando se pongan a disposición del titular los datos personales, o bien, mediante la expedición de copias simples, documentos electrónicos o cualquier otro medio que determine el responsable en el aviso de privacidad.

---

[407] INAI, *Guía para titulares de los datos personales*, [en línea] México, INAI, Vol. 3. Los derechos ARCO, s.a., [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://home.inai.org.mx/wp-content/documentos/GuiasTitulares/Guia%20Titulares-03_PDF.pdf* pp. 6-7.
[408] Artículo 29, LFPDPPP.

La entrega de los datos personales será gratuita, debiendo cubrir el titular únicamente los gastos justificados de envío o con el costo de reproducción en copias u otros formatos. El responsable podrá negar el acceso a los datos personales, o a realizar la rectificación o cancelación o conceder la oposición al tratamiento de los mismos, en los siguientes casos:

- Cuando el solicitante no sea el titular de los datos personales, o el representante legal no esté debidamente acreditado para ello.
- Cuando en su base de datos no se encuentren los datos personales del solicitante.
- Cuando se lesionen los derechos de un tercero.
- Cuando haya un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales.
- Cuando la rectificación, cancelación u oposición haya sido previamente realizada.

En caso de que el titular de los datos no reciba respuesta por parte del responsable, podrá iniciar una solicitud de protección de datos ante el INAI expresando con claridad el contenido de su reclamación y de los preceptos que considere vulnerados.

4.2.10.2 Procedimiento de Protección de Derechos ante el sector privado

Este procedimiento se presenta para atender las quejas en contra de las respuestas emitidas por responsables del sector privado a las solicitudes de ejercicio de derechos ARCO, o por falta de éstas.

La Guía para titulares de Datos Personales del INAI señala que el Procedimiento de Protección de Derechos (PPD) se puede originar por dos razones principales:[409]

1) Inconformidad con la respuesta que el responsable hubiese dado a una solicitud de ejercicio de derechos ARCO, o
2) Falta de respuesta del responsable a la solicitud de ejercicio de derechos ARCO.

Entre las causas que pueden motivar la inconformidad del titular con relación a la respuesta otorgada por el responsable se encuentran las siguientes:

- El responsable no otorgue acceso a los datos personales solicitados o lo haga en un formato incomprensible;
- El responsable se niegue a efectuar las rectificaciones a los datos personales;
- El titular no esté conforme con la información entregada por considerar que es incompleta o no corresponde a la solicitada, o bien, con el costo o modalidad de la reproducción;

[409] INAI, *Guía para Titulares de los Datos Personales,* [en línea] México, INAI, Vol. 4. Procedimientos de datos personales ante el INAI, s.a., [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://home.inai.org.mx/wp-content/documentos/GuiasTitulares/Guia%20Titulares-04_PDF.pdf* pp. 7-8.

- El responsable se niegue a cancelar los datos personales, y
- El responsable persista en el tratamiento a pesar de haber procedido la solicitud de oposición, o bien, se niegue a atender la solicitud de oposición.

Por tanto, para que proceda este procedimiento, será necesario que el titular de datos personales haya presentado previamente una solicitud de derechos ARCO ante el responsable.

Esquemáticamente, la guía esquematiza este procedimiento de la siguiente forma:[410]

[410] *Ibidem*. p. 11.

Imagen: Procedimiento de protección de derechos ante el sector privado.
Tomado de: *INAI, Guía para Titulares de los Datos Personales, Vol. 4. Procedimientos de datos personales ante el INAI,* México, INAI, s.a., [fecha de consulta: 4 de diciembre de 2022] Disponible en: https://idaip.org.mx/bibliotecadigital/product/guia-para-titulares-de-datos-personales-vol-4/ p.11.

4.2.10.3 Procedimiento de verificación administrativa

Es importante que los responsables tomen en consideración los derechos y obligaciones que tienen, de acuerdo con lo establecido en esta ley y que se han expuesto puntualmente en el presente artículo, ya que de no observar estas disposiciones pueden ser sujetos de alguna visita de verificación por parte de la autoridad administrativa, que en este caso es el INAI, el cual verificará el cumplimiento de la LFPDPPP.

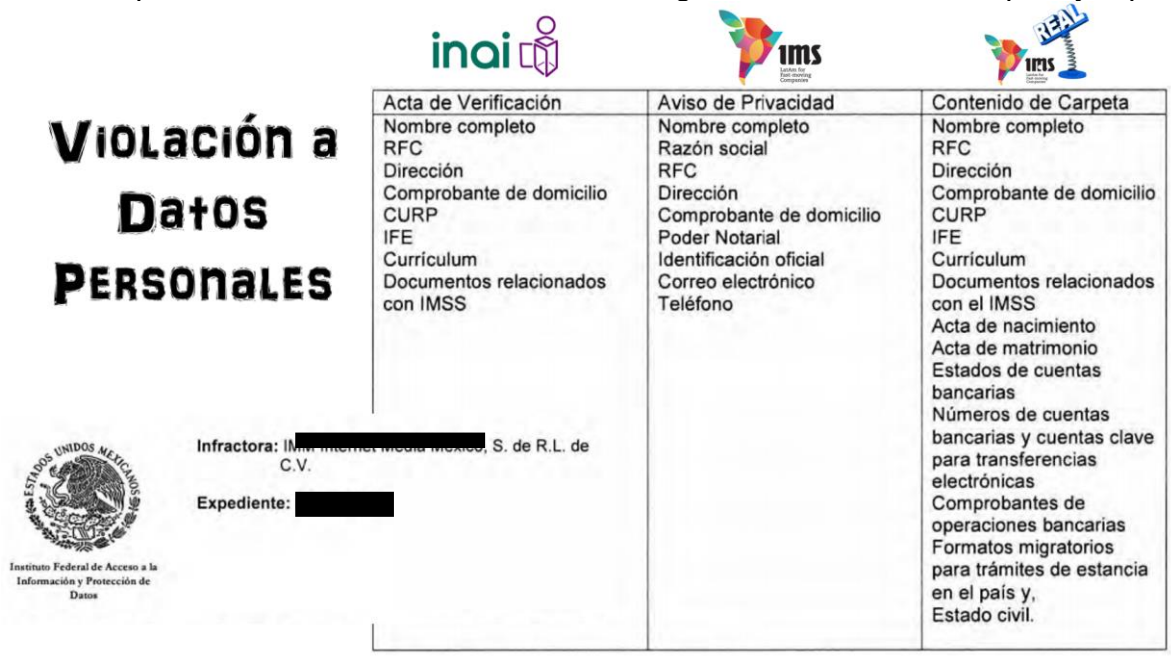
Cualquier persona podrá denunciar ante el INAI el indebido tratamiento de datos personales o presuntas violaciones a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, su Reglamento y demás normatividad aplicable.

Los procedimientos de investigación y verificación sólo aplican cuando un particular quiera denunciar un tratamiento indebido de datos personales por parte de un responsable del sector privado, lo que implica que el denunciante tenga conocimiento y pruebas de que el responsable está incumpliendo las disposiciones de la LFPDPPP, su Reglamento y demás normatividad aplicable, o no está tratando los datos personales respetando los principios y deberes.[411]
De manera esquemática el procedimiento es el siguiente:[412]

[411] *Ibidem*. p. 22.
[412] *Ibidem*. p. 25.

Imagen: Procedimiento de investigación ante el sector privado.
Tomado de: *INAI, Guía para Titulares de los Datos Personales, Vol. 4. Procedimientos de datos personales ante el INAI,* México, INAI, s.a., [fecha de consulta: 4 de diciembre de 2022] Disponible en: https://idaip.org.mx/bibliotecadigital/product/guia-para-titulares-de-datos-personales-vol-4/ p.25.

En estos procedimientos de verificación algo común es verificar el tratamiento de los datos personales, así como los niveles de seguridad en los mismos, por ejemplo:



Acta de Verificación	Aviso de Privacidad	Contenido de Carpeta
Nombre completo RFC Dirección Comprobante de domicilio CURP IFE Currículum Documentos relacionados con IMSS	Nombre completo Razón social RFC Dirección Comprobante de domicilio Poder Notarial Identificación oficial Correo electrónico Teléfono	Nombre completo RFC Dirección Comprobante de domicilio CURP IFE Currículum Documentos relacionados con el IMSS Acta de nacimiento Acta de matrimonio Estados de cuentas bancarias Números de cuentas bancarias y cuentas clave para transferencias electrónicas Comprobantes de operaciones bancarias Formatos migratorios para trámites de estancia en el país y, Estado civil.

Imagen: Investigación en el sector privado.
Fuente: Elaboración propia

En la imagen anterior, se puede apreciar en la primera columna, lo que el INAI fue a verificar, en la segunda columna, lo que la empresa contestó; y en la tercera, la batería real de datos que trataba la responsable. Como se puede apreciar, la empresa ni siquiera tenía una auditoría de datos completa.

En un caso que me tocó llevar en 2021, el INAI preguntó al responsable lo siguiente:

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

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOSPERSONALES

SECRETARIA DE PROTECCIÓN DE DATOS PERSONALES
DIRECCIÓN GENERAL DE INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PRIVADO

EXPEDIENTE: I[redacted]/2021

OFICIO: INAI/S[redacted]43/21
ASUNTO: Requerimiento

Ciudad de México, a 16 de abril del 2021.

siguiente información, debiendo anexar copia de la documentación con que cuente para probar su dicho:

1. Acredite fehacientemente la forma en que su representada dio a conocer a la denunciante su Aviso de Privacidad.
2. Acredite fehacientemente la forma en que la Denunciante otorgó su consentimiento para el tratamiento de sus datos personales.
3. Remita la documentación que acredite la implementación de medidas para garantizar el debido tratamiento de los datos personales en términos de lo dispuesto en el artículo 48 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Imagen: Procedimiento de investigación ante el sector privado (caso de estudio).
Fuente: Elaboración propia a partir de un procedimiento real ante el INAI.

De lo anterior se aprecia que actualmente el INAI pide “fehacientemente” que se acredite la forma en que los responsables protegen los datos personales, recaban consentimiento, así como las medidas de seguridad que tiene implementadas.

4.2.11 Autoridades administrativas

En materia administrativa, el INAI es la autoridad garante de proteger los datos en poder de los particulares, constituyéndose como la autoridad administrativa encargada de interpretar esta ley, de emitir criterios y recomendaciones a efecto de proteger el derecho a la protección de datos personales, así como de divulgar estándares y mejores prácticas internacionales en materia de seguridad de la información.

Por su parte, la Secretaría de Economía tendrá como función difundir el conocimiento de las obligaciones en torno a la protección de datos personales entre la iniciativa privada nacional e internacional con actividad comercial en territorio mexicano; también de promover las mejores prácticas comerciales en torno a la protección de los datos personales como insumo de la economía digital, y el desarrollo económico nacional en su conjunto. En lo referente a las bases de datos de comercio, la regulación únicamente será aplicable a las bases de datos

automatizadas o que formen parte de un proceso de automatización.

Es importante destacar que, de acuerdo con la LFPDPPP, en su artículo 56, dispone expresamente: Contra las resoluciones del Instituto, los particulares podrán promover el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa. Sin embargo, en 2020 se resolvió una contradicción de tesis por parte de la segunda sala de la SCJN la cual se coloca a continuación por su importancia y trascendencia en este tema:

> **JUICIO CONTENCIOSO ADMINISTRATIVO FEDERAL. ES IMPROCEDENTE CONTRA LAS RESOLUCIONES EMITIDAS POR EL INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES (INAI), EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE PARTICULARES.**[413]
>
> Criterios discrepantes: Los Tribunales Colegiados contendientes analizaron si las resoluciones que emite el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), en materia de protección de datos personales en posesión de particulares, son impugnables a través del juicio contencioso administrativo ante el Tribunal Federal de Justicia Administrativa, en términos del artículo 56 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, llegando a soluciones contrarias.
>
> Criterio jurídico: La Segunda Sala de la Suprema Corte de Justicia de la Nación decide que el juicio de nulidad es improcedente, porque de acuerdo con la reforma constitucional publicada en el Diario Oficial de la Federación el 7 de febrero de 2014, la única vía para combatir estas resoluciones es el juicio de amparo.
>
> Justificación: Es así, porque uno de los objetivos esenciales de la aludida reforma constitucional en materia de transparencia, fue que los particulares únicamente pudieran impugnar las resoluciones de dicho Instituto vía juicio de amparo, con la clara intención de no alargar los procedimientos en materia de acceso a la información y tutelar de mejor manera ese derecho; en ese sentido, si el Poder Reformador de la Constitución otorgó competencia al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales para conocer de la materia de protección de datos personales en posesión de los particulares, en tanto se determina la instancia responsable encargada de atender los temas en esa materia, debe entenderse derogado el artículo 56 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, porque al ser de contenido previo a la mencionada reforma, resulta contrario al marco constitucional y legal que lo rige en la actualidad, conforme al cual los particulares sólo pueden impugnar sus resoluciones a través del juicio de amparo.

[413] Tesis: 2a./J. 31/2020 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. I, octubre de 2020, p. 668.

4.2.12 Infracciones y Sanciones

Las infracciones a la presente ley serán sancionadas por el INAI con:

1) Apercibimiento, tratándose de incumplimiento de la solicitud del titular sin razón fundada.
2) Multa de 100 a 160,000 días de salario mínimo general vigente en la CDMX (Hoy en UMAS), en los casos siguientes:
    a. Actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso.
    b. Actuar en contravención a los principios de la ley.
    c. Declarar dolosamente la inexistencia de datos personales.
    d. Omitir en el aviso de privacidad, alguno o todos sus elementos.
    e. Mantener datos personales inexactos cuando resulte imputable al responsable, o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de los titulares.
    f. Incumplir con el apercibimiento del INAI.
3) Multa de 200 a 320,000 días de SMGDF, en los siguientes casos:
    a. Incumplir el deber de confidencialidad.
    b. Cambiar sustancialmente la finalidad originaria del tratamiento de los datos.
    c. Transferir datos a terceros sin comunicar a éstos el aviso de privacidad.
    d. Vulnerar la seguridad de bases de datos, locales, programas o equipos.
    e. Por la transferencia o cesión de los datos personales, cuando no estén permitidos por la ley.
    f. Recabar o transferir datos personales sin el consentimiento expreso del titular.
    g. Obstruir los actos de verificación de la autoridad.
    h. Recabar datos en forma engañosa y fraudulenta.
    i. Continuar con el uso ilegítimo de los datos personales cuando se ha solicitado el cese del mismo por el INAI o los titulares.
    j. Afectar o impedir el ejercicio de los derechos ARCO.
    k. Crear bases de datos en contravención a la ley.

Cabe destacar que la ley contiene un capítulo específico sobre delitos derivados del tratamiento indebido de datos personales en los siguientes supuestos:

1) Cuando el responsable autorizado para tratar datos personales provoque una vulneración de seguridad a las bases de datos bajo su custodia con ánimo de lucro, la sanción será de tres meses a tres años de prisión.
2) Cuando el responsable trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos con el fin de alcanzar un lucro indebido, la sanción será de seis meses a cinco años de prisión.

En la página del INAI se pueden encontrar la tabla de las multas impuestas por el Instituto y pagadas por los infractores, ante la autoridad recaudadora, con base en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares[414], la cual se va actualizando periódicamente.

SECTOR INDUSTRIAL:	IMPORTE TOTAL MULTA IMPUESTA AL SECTOR	IMPORTE MULTA PAGADA
Servicios Financieros y de Seguros	$265,988,638.10	$36,424,892.37
Servicios de Salud y de Asistencia Social	$18,032,529.16	$5,122,191.00
Transportes, Correos y Almacenamiento	$8,545,562.50	$4,306,560.00
Información en Medios Masivos	$66,459,505.10	$5,530,586.00
Industrias Manufactureras	$9,788,360.99	$131,269.00
Servicios Profesionales, Científicos y Técnicos	$13,722,143.42	$20,399.00
Comercio al Por Menor	$36,690,849.83	$140,524.50
Servicios de Esparcimiento Culturales y Deportivos, y Otros Servicios Recreativos	$17,210,059.00	$0.00
Servicios Educativos	$17,744,197.12	$0.00
Servicios de Apoyo a los Negocios y Manejo de Residuos y Desechos, y Servicios de Remediación	$19,337,840.55	$0.00
Comercio al Por Mayor	$2,955,713.18	$0.00
Servicios de Alojamiento Temporal y de Preparación de Alimentos y Bebidas	$2,733,956.00	$0.00
Servicios Inmobiliarios y de Alquiler de Bienes Muebles e Intangibles	$5,551,093.00	$43,077.00
Otros Servicios Excepto Actividades Gubernamentales	$550,879.00	$0.00
No Disponible	$384,244.00	$0.00

[414] INAI, *Multas impuestas por el Instituto y pagadas por los infractores, ante la autoridad recaudadora, con base en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, México, INAI, 2022, [fecha de consulta: 4 de diciembre de 2022] Disponible en: *https://home.inai.org.mx/?page_id=3456*

SECTOR INDUSTRIAL:	IMPORTE TOTAL MULTA IMPUESTA AL SECTOR	IMPORTE MULTA PAGADA
Agricultura, Cría y Explotación de Animales, Aprovechamiento Forestal, Pesca y Caza	$22,668.00	$0.00
Construcción	$10,135,239.00	$0.00
Corporativos	$604,500.00	$0.00
Generación, Transmisón y Distribución de Energía Eléctrica, Suministro de Agua y de Gas por Ductos al Consumidor Final	$0.00	$0.00
Minería	$0.00	$0.00
TOTAL	**$496,457,977.95**	**$51,719,498.87**

INFRACTOR	SECTOR	IMPORTE MULTA IMPUESTA	IMPORTE MULTA PAGADA
BUHOLEGAL S. DE R.L. DE C.V.	SERVICIOS PROFESIONALES, CIENTÍFICOS Y TÉCNICOS	$20,399.00	$20,399.00
CREACIONES TEXTILES DE MÉRIDA, S.A. DE C.V.	INDUSTRIAS MANUFACTURERAS	$129,520.00	$131,269.00
BANCO MERCANTIL DEL NORTE, S.A., INSTITUCIÓN DE BANCA MÚLTIPLE, GRUPO FINANCIERO BANORTE	SERVICIOS FINANCIEROS Y DE SEGUROS	$32,006,691.00	$36,424,892.37
COMUNICACIONES NEXTEL DE MÉXICO, S.A. DE C.V.	INFORMACIÓN EN MEDIOS MASIVOS	$4,241,780.00	$4,462,352.00
CONCESIONARIA VUELA COMPAÑÍA DE AVIACIÓN, S.A.P.I. DE C.V. (VOLARIS)	TRANSPORTES, CORREOS Y ALMACENAMIENTO	$4,306,560.00	$4,306,560.00
IMPULSE TELECOMMUNICATIONS DE MÉXICO, S.A. DE C.V.	INFORMACIÓN EN MEDIOS MASIVOS	$942,060.00	$1,068,234.00

INFRACTOR	SECTOR	IMPORTE MULTA IMPUESTA	IMPORTE MULTA PAGADA
OPERADORA DE HOSPITALES ANGELES, S.A. DE C.V.	SERVICIOS DE SALUD Y DE ASISTENCIA SOCIAL	$4,601,520.00	$4,601,520.00
STAR MÉDICA, S.A. DE C.V.	SERVICIOS DE SALUD Y DE ASISTENCIA SOCIAL	$474,760.00	$482,926.00
BALCASA CONSULTORES, S.C.	SERVICIOS INMOBILIARIOS Y DE ALQUILER DE BIENES MUEBLES E INTANGIBLES	$42,060.00	$43,077.00
REPRESENTACIONES GG, S.A DE C.V.	COMERCIO AL POR MENOR	$94,362.50	$94,362.50
TIK TEK PHARMACEUTICS, S. DE R.L. DE C.V.	COMERCIO AL POR MENOR	$15,098.00	$15,480.00
GOT MUEBLES, S.A. DE C.V.	COMERCIO AL POR MENOR	$30,196.00	$30,682.00
CLÍNICA DE SERVICIOS MÉDICOS COLIMAN, S.A. DE C.V.	SERVICIOS DE SALUD Y DE ASISTENCIA SOCIAL	$37,745.00	$37,745.00
		$46,942,751.50	**$51,719,498.87**

Capítulo 5. Retos en Materia de Transparencia, y Datos Personales

5.1 Retos Comunes entre el Acceso a la Transparencia y la Protección de Datos Personales

5.1.1. Interacción entre sistemas Transparencia y Datos Personales con otros sistemas

Como se ha visto a lo largo de este trabajo, las leyes generales de naturaleza administrativa, han creado una serie de sistemas nacionales: Educación, Salud, Asentamientos Humanos, Deporte, Seguridad Pública, Anticorrupción, Transparencia, Datos Personales, Medio Ambiente; etc.

Abordaré este punto de interacción desde el punto de vista físico-biológico, donde considero que la interacción se puede observar desde dos modelos igualmente válidos:

1) Mecanicista-independiente.
2) Integrador como sistema de entrelazamiento.

Digo que igualmente válidos, porque el observador (operador de la norma, juez, autoridad, sujeto obligado, particular; etc.) va a ver lo que quiere ver, es decir, ver el sistema desde un punto de vista independiente; o bien, desde un punto de vista integrador y de aplicación homogénea.

Desde el modelo mecanicista-independiente tenemos un gran sistema que es el Sistema Normativo Nacional, y los demás sistemas tendrían la naturaleza de subsistemas. En este sentido, cada subsistema actúa como una esfera independiente que fluyen y confluyen como partículas que van de aquí para allá, que chocan y actúan.

Aquí, el subsistema de Transparencia, Acceso a la Información y Datos Personales (Transparencia y Datos Personales) actúa como una esfera única que interrelaciona con otros subsistemas, desarrollando sus propios principios y reglas. En este sentido, actúa como un subsistema más dentro de nuestro sistema normativo nacional.

Considero que uno de los retos más significativos desde este punto de vista es el de la interrelación de sistemas, ya que, viéndolo desde el punto de vista de sus elementos, tenemos subsistemas independientes como el de Transparencia y Datos Personales, Anticorrupción, Seguridad Pública, Salud, etc.

En este punto de vista, cada sistema, además de desarrollar de manera separada sus reglas y principios, podrían actuar como partículas sin mucho orden, a veces chocando entre ellas, generando entropía (caos) o bien, invadiendo esferas.

Esquemáticamente, lo podríamos ver de la siguiente forma:

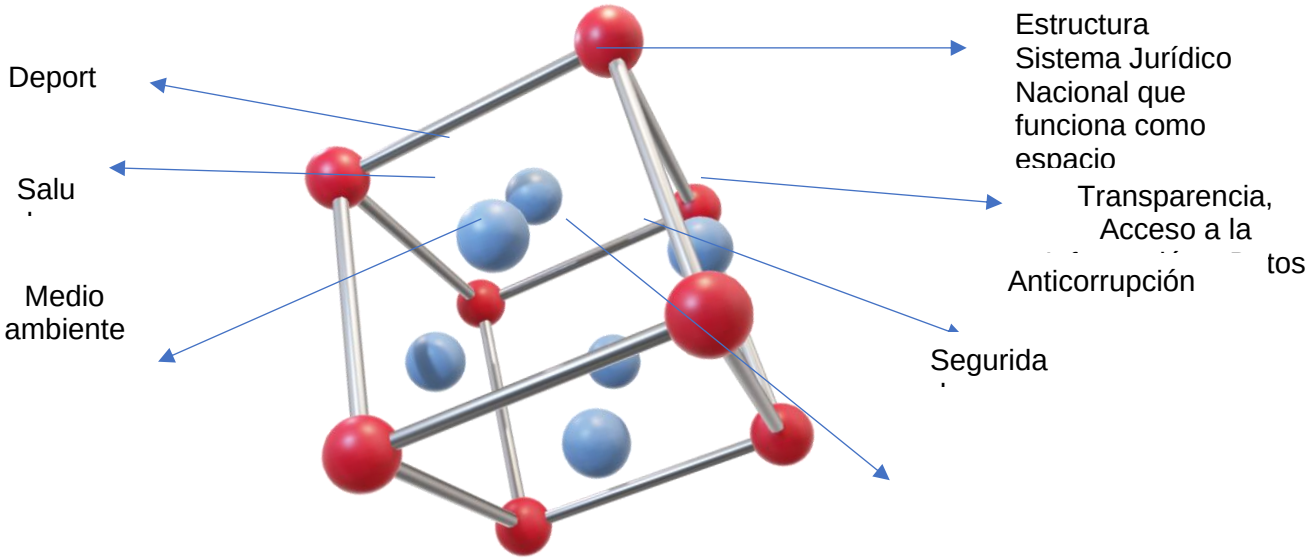


Imagen: Relación normativa de Leyes Generales en México.
Fuente: Elaboración propia.

Con cada creación de ley general, se agrega una esfera-sistema adicional, con sus propias, reglas, principios, procedimientos, etc.

En este esquema, todas las leyes forman parte del uno; donde la Constitución es el gran uno, y la Ley General que es una ley reglamentaria de precepto constitucional, es una parte del todo, el cual genera un nuevo sistema que crea relaciones de coordinación, concurrencia y colaboración entre los órdenes de gobierno.

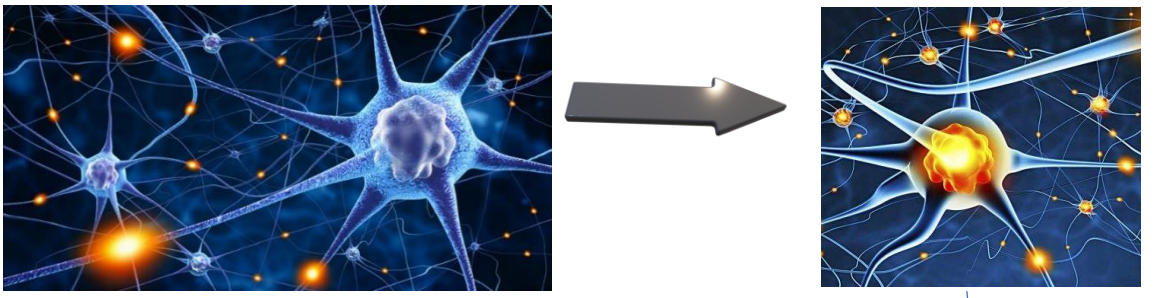
Ahora bien, si cambiamos el punto de vista del observador, el esquema arriba planteado, genera un planteamiento: ¿qué mantiene unidos a los sistemas?

Desde el punto de vista mecanicista, podemos ver que existe una especie de vacío y cada sistema es una partícula sin ningún tipo de relación aparente; sin embargo, si dejamos de ver a la Transparencia y Protección de Datos como una partícula autónoma y lo vemos desde el punto de vista de la transversalidad entonces aparece la integración.

Por otra parte; desde un punto de vista más integrador, el sistema de Transparencia y Datos Personales pasaría a ser un sistema de entrelazamiento el cual proporciona una forma de unir a los demás sistemas; como un mecanismo de equilibrio, control y cohesión.

Bajo este modelo, tanto la transparencia, como los datos personales, pueden ingresar completamente en cada uno de los sistemas actuando como una red neuronal, tal como se aprecia en las siguientes imágenes:

Sistema Normativo (Deporte, salud, Seguridad, Anticorrupción, etc.)



https://www.caracteristicas.co/neuronas/

https://www.funcion.info/neuronas/

Transparencia y Protección de Datos

Transparencia y Protección de Datos integrándose con un Sistema Normativo

Imagen: Estructura neuronal de un sistema normativo a partir de un sistema orgánico.
Fuente: Elaboración propia.

Bajo este modelo, si bien, cada sistema tiene una realidad aplicativa independiente, se encuentran unidas por un nexo común donde todos sistemas existen y coexisten, por lo que mucho dependerá del observador y aplicador de la norma.

Independientemente de estos dos puntos de vista, ninguno de los sistemas es perfecto, ya que son operados por humanos y de ahí que el factor humano influirá en la aplicación normativa. No es perfecto porque los sistemas evolucionan con el devenir del tiempo; así como por acontecimientos sociales, económicos, políticos, ambientales o de cualquier otro.

5.1.2 Evolución tecnológica en el ejercicio de Transparencia, Acceso a la Información y Datos Personales en Posesión de Sujetos Obligados.

Ha pasado ya tiempo desde que apareció en funciones el Sistema de Solicitudes de Información (2003) del entonces Instituto Federal de Acceso a la Información Pública. El pasado 13 de septiembre de 2021, inició operaciones el Sistema de Solicitudes de Acceso a la Información (SISAI 2.0) de la Plataforma Nacional de Transparencia (PNT).

Lo anterior, marca un espacio de 3 (tres) sistemas informáticos diferentes para el ejercicio de los derechos de transparencia, acceso a la información y protección de datos personales de los ahora denominados sujetos obligados.

De igual forma, el cambio en la forma de facilitar la información en la plataforma del INAI ha ido cambiando con el fin de ser más intuitiva y fácil de manejar.

No obstante, los claroscuros siempre estarán en combatir la brecha tecnológica y digital en la que nos encontramos; donde por una parte con ciudadanos cada vez más digitalizados pueden buscar información, ejercer derechos ARCOP[415], coadyuvar con la rendición de cuentas y transparencia proactiva. Y por otro lado ciudadanos sin siquiera saber los mínimos derechos, como el caso de población de ejidos y comunidades.

Ya decía Enrique Dans, que "si algo define a la especie humana es la tecnología".[416] Es un hecho que la tecnología transforma nuestro mundo y cada vez los cambios son más y más acelerados gracias a todas las tecnologías de la información aplicadas en este caso a la transparencia (acceso a la información, rendición de cuentas, archivos) y datos personales.

Organismos como el INEGI, estarán dando cuenta gracias a sus estadísticas, como es la percepción de la transparencia, acceso a medios electrónicos y otras estadísticas que deberían ser consideradas por los órganos garantes, para mejorar y diseñar estrategias de difusión más efectivas para dar a conocer el acceso a la información.

Finalmente, el pasado 25 de febrero de 2022, se publicó en el Diario Oficial de la Federación el Acuerdo mediante el cual se aprueba la habilitación de la herramienta en línea INAI-EIPDP como medio para la presentación de los procedimientos establecidos en las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales.

Según este acuerdo, de conformidad con lo dispuesto en el artículo 74 de la Ley General de Datos, el responsable que 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.

La plataforma en línea INAI-EIPDP servirá como medio para la presentación de los procedimientos establecidos en las disposiciones administrativas, que funcionará como un portal informativo y transaccional, que permitirá cumplir con los requisitos previstos por los artículos 3, fracción XVI, 74, primer párrafo, 75, 77, 78 y 79 de la

[415] Al ejercicio de los derechos ARCO se agrega el de portabilidad de datos.
[416] Dans, Enrique, *Viviendo en el Futuro. Claves sobre cómo la tecnología está cambiando nuestro mundo,* [en línea] España, Planeta-Deusto, 2019, [fecha de consulta: 5 de diciembre de 2022] Disponible en:
https://www.planetadelibros.com/libros_contenido_extra/42/41488_Viviendo_en_el_futuro.pdf p. 21.

LGPDPPSO, así como en las disposiciones administrativas, poniendo a disposición de los responsables del sector público, una herramienta en línea para la sistematización de la tramitación de evaluaciones de impacto en la protección de datos personales, consultas relacionadas con su presentación y gestión de informes de exención.

5.2. Retos en Materia de Transparencia, Acceso a la Información y Rendición de cuentas.

5.2.1. Combate a la Corrupción

Ha quedado claro que la corrupción constituye uno de los más grandes cánceres en la sociedad, y con toda responsabilidad y sin temor a equivocarme, es un fenómeno que jamás podrá ser erradicado. Sin embargo, el panorama no debe ser totalmente fatalista, la transparencia ha venido a ser una especie de tratamiento para controlar y disminuir la opacidad y malas prácticas de ocultamiento o negación de información.

Actualmente, contamos con el Programa Nacional de Combate a la Corrupción y a la Impunidad, y de Mejora de la Gestión Pública 2019-2024, (DOF: 30/08/2019), el cual constituye el último esfuerzo en la materia. Este Programa tiene 5 grandes objetivos prioritarios:

Objetivos prioritarios del Programa Nacional de Combate a la Corrupción y a la Impunidad, y de Mejora de la Gestión Pública 2019-2024
1.- Combatir frontalmente las causas y efectos de la corrupción
2.- Combatir los niveles de impunidad administrativa en el Gobierno Federal
3.- Promover la eficiencia y eficacia de la gestión pública
4.- Promover la profesionalización y la gestión eficiente de los recursos humanos de la Administración Pública Federal
5.- Promover el uso eficiente y responsable de los bienes del Estado Mexicano

De este programa destaca la falta de colaboración con los otros poderes, lo más que se le encuentra es la estrategia prioritaria 3.4.2 Fortalecer la oferta de capacitación en materia de seguimiento, monitoreo, evaluación, rendición de cuentas y transparencia en los servidores públicos de los tres poderes y órdenes de gobierno.

El Senado de la República cuenta con la Comisión de Anticorrupción y Participación Ciudadana, la cual tiene como encomienda participar en la formulación, discusión, análisis y participación en la instrumentación del marco legal, referente a la prevención y combate a la corrupción, en los diferentes órdenes de gobiernos, así como sus controles transversales mediante la transparencia y la rendición de cuentas gubernamental.[417]

[417] *Cfr*. Senado de la República, *Bienvenida*, [en línea], México, Senado de la República, Comisión de Anticorrupción y Participación Ciudadana, [fecha de consulta: 5 de diciembre de 2022] Disponible

Resalta ver que la última iniciativa presentada fue en 2018; por lo que hace a reuniones de trabajo, la última reunión de trabajo presentada es en mayo de 2018. En sus foros y conferencias reportadas, se aprecia como último foro y conferencia el año de 2017. A mi parecer, hace falta mucho trabajo efectivo de esta Comisión.

En el caso de la Cámara de Diputados Federal, también cuenta con una Comisión de Transparencia y Anticorrupción, la cual "es uno de los órganos constituidos por el Pleno en el Palacio Legislativo, que, a través de la elaboración de dictámenes, informes, opiniones o resoluciones, contribuye a que la Cámara de Diputados cumpla sus atribuciones constitucionales y legales."[418]

De manera similar a la Cámara de Senadores, tienen un rezago desde 2018; incluso en sus programas anuales publicados también aparece como último, el de 2018.

El Poder Judicial si bien, forma parte del Sistema Nacional Anticorrupción, no cuenta con una página que condense adecuadamente los instrumentos que ha generado al interior del mismo. De hecho, la Política Nacional Anticorrupción aprobada el 29 de enero de 2020 por el Comité Coordinador del Sistema Nacional Anticorrupción, indica que una de las principales causas de la corrupción es: "Poder judicial ineficaz que no rinde cuentas tanto a nivel federal como en las entidades federativas".[419] Considero que actualmente el lenjuage de la anticorrupción son más palabras que acciones concretas. En este sentido, la transparencia ayuda a encontrar huecos en informes, falta de estándares en la información relativa al tema, de las cuales se pueden fomentar acciones.

5.2.2. Clasificación y desclasificación de la información

Con la nueva Ley General de Transparencia, se da un nuevo giro en la forma por medio de cual se debe realizar la clasificación de la información. Independientemente que se cuenten con los mecanismos e instrumentos para realizar dicha clasificación, podrían existir externalidades en la parte de emitir decretos "velados" que impliquen una clasificación *a priori*.

Cuando me refiero a clasificación "velada" me refiero al reciente acuerdo publicado en el DOF el pasado 22 de noviembre de 2021, por el cual se instruye a las dependencias y entidades de la Administración Pública Federal a realizar las acciones que se indican, en relación con los proyectos y obras del Gobierno de México considerados de interés público y seguridad nacional, así como prioritarios y estratégicos para el desarrollo nacional.

---

en: *https://www.senado.gob.mx/comisiones/anticorrupcion/index.php*

[418] Cámara de Diputados, *Bienvenido*, [en línea], México, Cámara de Diputados, Comisión de Transparencia y Anticorrupción, s.a., [fecha de consulta: 5 de diciembre de 2022] Disponible en: *http://www5.diputados.gob.mx/index.php/camara/Comision-de-Transparencia-y-Anticorrupcion*

[419] Secretaría Ejecutiva del sistema Nacional Anticorrupción, *Política Nacional Anticorrupción*, [en línea] México, SESNA, 2020, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://www.sesna.gob.mx/wp-content/uploads/2020/02/Pol%C3%ADtica-Nacional-Anticorrupci%C3%B3n.pdf* p. 34.

Este decreto fue tan controvertido que el mismo 10 de diciembre de 2021, el INAI ingresó una demanda de controversia constitucional contra este decreto, por medio de la cual se señalaron como efectos negativos del acuerdo reclamado:

> En cuanto a la parte dispositiva, el Acuerdo contiene una clasificación anticipada, generalizada y definitiva, respecto de la información que se produzca en la realización de ellos proyectos y las obras a cargo del Gobierno de México señalados en su artículo Primero, puesto que los declara de interés público y seguridad nacional, con lo que clasifica como reservada toda la información que se origine en dichos proyectos, siendo una clasificación ex ante y general que no distingue entre cierta información y otra, por lo que se concluye que toda gozará de la misma naturaleza, es decir, reservada. […]
>
> Ahora bien, se considera que el mensaje que emite el Acuerdo impugnado se encuentra relacionado con un régimen de opacidad y secreto que no se ajusta a las directrices establecidas para la aplicación de excepciones al derecho de acceso a la información. Es decir, la utilización de dicho vocablo tiene una aplicación transversal en diversas materias, incluyendo la relativa al acceso a la información.
>
> De tal forma que el Acuerdo impugnado realiza una reserva de la información por motivos de seguridad nacional e interés público y que, por disposición implícita y explícita, será causa jurídica y fundamento de posteriores actos individualizados de reserva, con lo cual se conculca el derecho de acceso a la información pública, que el INAI tiene el deber constitucional de garantizar.[420]

Pero esto es solo la primera parte del problema, la segunda parte, va en lo referente a la desclasificación de información. Si bien el 15 de abril de 2016 se publicó en el DOF el acuerdo del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, por el que se aprueban los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas en el ámbito federal; en cada entidad federativa se han emitido lineamientos de clasificación y desclasificación.

En este sentido, creo que aún estamos en zona de aprendizaje respecto a la clasificación de la información aplicando la prueba de daño, y que aun tardaremos algunos años más para emitir acuerdos de desclasificación de información.

[420] INAI, *Demanda de Controversia Constitucional*, [en línea] México, INAI, 2021, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Controversia%20Constitucional%20101221.pdf* p. 37.

5.2.3 Sistemas de Archivos

La nueva Ley General de Archivos publicada el 15 de junio de 2018 se establece un nuevo sistema, denominado Sistema Nacional de Archivos, que viene a complementar y formar parte del Sistema Nacional de Transparencia, el cual tendrá un órgano de coordinación denominado Consejo Nacional, mismo que instaló su primera sesión ordinaria el 25 de septiembre de 2020.

Este Consejo Nacional deberá:[421]

1) Aprobar y difundir la normativa relativa a la gestión documental y administración de archivos, conforme a las mejores prácticas de la materia;
2) Aprobar y difundir los criterios y plazos para la organización y conservación de los archivos que permitan localizar eficientemente la información pública;
3) Formular recomendaciones archivísticas para la emisión de normativa para la organización de expedientes judiciales;
4) Emitir recomendaciones a los sujetos obligados para aplicar la Ley en sus respectivos ámbitos de competencia;
5) Aprobar los lineamientos que establezcan las bases para la creación y uso de sistemas automatizados para la gestión documental y administración de archivos, que contribuyan a la organización y administración homogénea de los archivos de los sujetos obligados;
6) Aprobar acciones de difusión, divulgación y promoción sobre la importancia de los archivos como fuente de información esencial, del valor de los datos abiertos de los documentos de archivo electrónico y como parte de la memoria colectiva;
7) Aprobar la política nacional de gestión documental y administración de archivos;
8) Promover entre los tres órdenes de gobierno, estrategias de difusión y divulgación del trabajo archivístico, del patrimonio documental y patrimonio documental de la Nación.

5.2.4. Participación de la ciudadanía

Las organizaciones de la sociedad civil desempeñan un papel fundamental en la promoción y defensa de la transparencia, la rendición de cuentas y el ejercicio del derecho a saber. Constituyen un contrapeso, ante el poder público, para generar las condiciones de una sociedad más participativa, democrática y con mejor calidad de vida.[422]

---

[421] Artículo 67, Ley General de Archivos.

[422] Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, *Organizaciones de la Sociedad Civil*, INFOCDMX, [en línea], México, InfoCDMX, s.a., [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://infocdmx.org.mx/index.php/transparencia-en-m%C3%A9xico/organizaciones-de-la-sociedad-civil.html#:~:text=Las%20organizaciones%20de%20la%20sociedad,ejercicio%20del%20derecho%20a%20saber.&text=Iniciativa%20Ciudadana%20y%20Desarrollo%20Social%20%2D%20INCIDE%20Social%20A.C.*

Se pueden mencionar algunas OSC entre ellas:[423]

Imagen: Organizaciones de la Sociedad Civil que trabajan en materia de Transparencia en la Ciudad de México
Tomado de: INFOCDMX *Organizaciones de la Sociedad Civil*, [en línea], México, InfoCDMX, s.a., [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://infocdmx.org.mx/index.php/transparencia-en-m%C3%A9xico/organizaciones-de-la-sociedad-civil.html#:~:text=Las%20organizaciones%20de%20la%20sociedad,ejercicio%20del%20derecho%20a%20saber.&text=Iniciativa%20Ciudadana%20y%20Desarrollo%20Social%20%2D%20INCIDE%20Social%20A.C*.

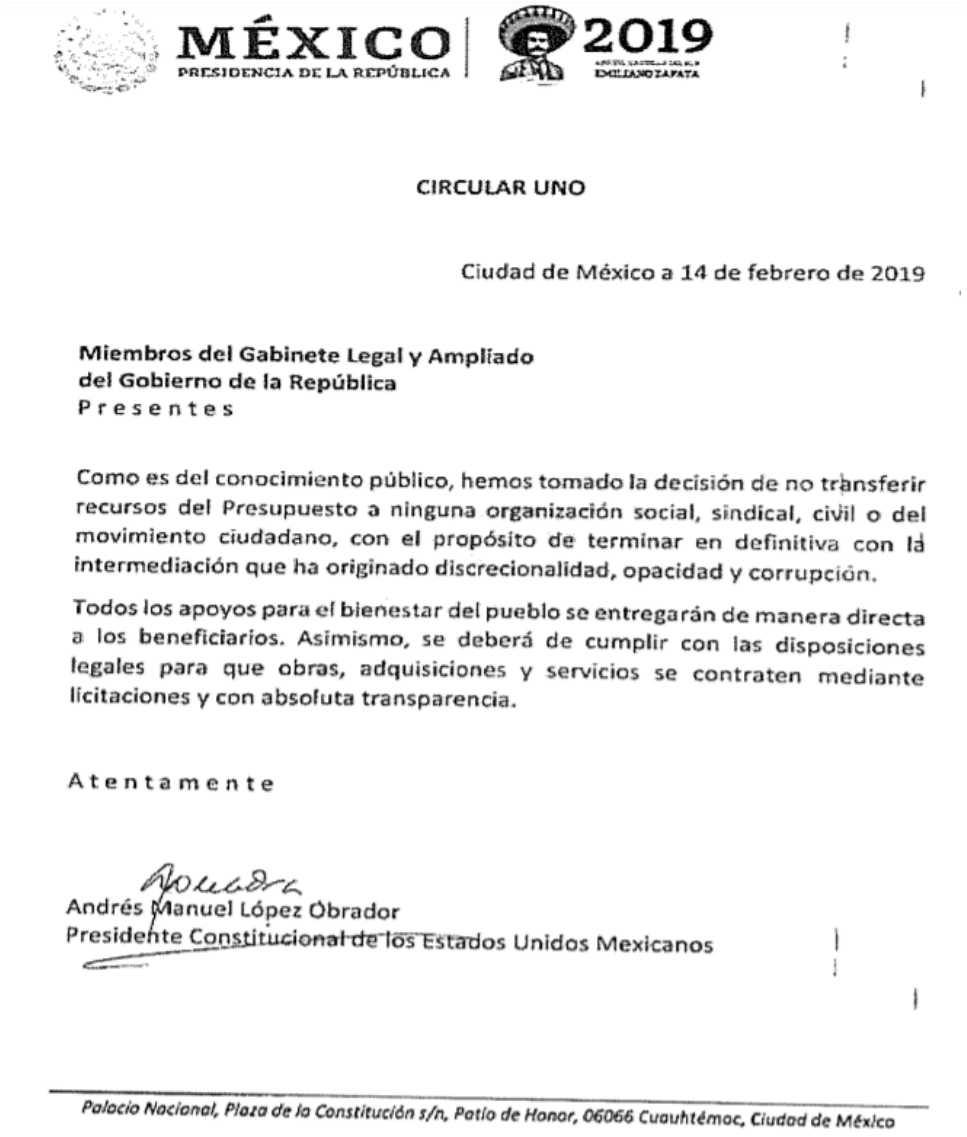
Como se sabe muchas de estas organizaciones necesitan recursos para fondear sus proyectos, algunas de ellas presentaban solicitudes de recursos al entonces Instituo Nacional de Desarrollo Social (INDESOL). En 2015 se emitió una convocatoria denominada Iniciativas Ciudadanas en materia de acceso a la información pública y protección de datos personales (AI), de la cual tuve la oportunidad se evaluar algunos proyectos.

Dicha convocatoria tenía como objetivos:

1) Desarrollar proyectos con OSC para extender el ejercicio de los derechos de acceso a la información y protección de datos personales.
2) Impulsar estrategias en conjunto con asociaciones civiles, para que la población se apropie de estos derechos.
3) Promover el intercambio de experiencias y prácticas exitosas entre OSC que incidan en estas temáticas, para socializar sus resultados, metodologías, propuestas y recomendaciones. Así como fomentar la réplica de estrategias o incidencia en el mejoramiento y fortalecimiento de programas y prácticas sociales específicas.[424]

[423] *Ídem*.
[424] Instituto Nacional de Desarrollo Social, *Indesol e Inai lanzan convocatoria a OSC de todo el país*,[en línea], México, INDESOL, 29 de julio de 2015, [fecha de consulta: 5 de diciembre de 2022]

No obstante, el pasado 14 de febrero de 2019 y cual “regalo del día del amor y la amistad” el jefe del Ejecutivo Federal emitió la Circular UNO la cual indicó la decisión de “no transferir recursos del Presupuesto a ninguna organización social…”. A continuación el texto de dicho documento:[425]



MÉXICO
PRESIDENCIA DE LA REPÚBLICA
2019
EMILIANO ZAPATA

CIRCULAR UNO

Ciudad de México a 14 de febrero de 2019

Miembros del Gabinete Legal y Ampliado
del Gobierno de la República
Presentes

Como es del conocimiento público, hemos tomado la decisión de no transferir recursos del Presupuesto a ninguna organización social, sindical, civil o del movimiento ciudadano, con el propósito de terminar en definitiva con la intermediación que ha originado discrecionalidad, opacidad y corrupción.

Todos los apoyos para el bienestar del pueblo se entregarán de manera directa a los beneficiarios. Asimismo, se deberá de cumplir con las disposiciones legales para que obras, adquisiciones y servicios se contraten mediante licitaciones y con absoluta transparencia.

Atentamente

Andrés Manuel López Obrador
Presidente Constitucional de los Estados Unidos Mexicanos

Palacio Nacional, Plaza de la Constitución s/n, Patio de Honor, 06066 Cuauhtémoc, Ciudad de México

No obstante a esta circular, la sociedad civil seguirá teniendo un rol importante en este sexenio y en los próximos seguramente ya que su actuación es fundamental en la formación de políticas públicas y de opinión sobre temas como la corrupción, la transparencia de presupuestos públicos, la rendición de cuentas, seguimientos de obras públicas, evaluación de políticas públicas, ejercer control social de la función pública, entre otros.

Disponible en: *https://www.gob.mx/indesol/prensa/indesol-e-inai-lanzan-convocatoria-a-osc-de-todo-el-pais*

[425] s/d. *https://reunionnacional.tecnm.mx/RND_2019/sa/CIRCULAR%20UNO.pdf*

5.3 Retos en Materia de Datos personales

5.3.1. Retos Comunes entre Sujetos Obligados y entre Particulares

A consideración del que esto escribe, considero que el reto común en materia de datos personales tanto para sujetos obligados como para particulares, es la de homologar determinados conceptos generales en beneficio de los titulares de Datos Personales tales como: principios rectores, derechos ARCO o ARCOP , así como procedimientos ante organismos garantes.

En este sentido, el INAI ha emitido documentos de forma física como interactiva sobre cuatro ejes principales:[426]

1. Conceptos generales de la protección de datos personales.
2. Principios rectores de la protección de datos personales.
3. Los derechos ARCO.
4. Procedimientos de datos personales ante el INAI.

Por su parte los organismos garantes en materia local, también emiten y actualizan en sus sitios web y sus micrositios de capacitación y publicaciones, material diverso en materia de protección y seguridad de datos personales.
Algunos de los temas en materia de datos personales que convergen en las esferas de sujetos obligados como de particulares están los siguientes:

1) Prevención de Robo de Identidad
2) Seguridad en el entorno Digital
3) Manejo de Redes Sociales
4) Supervisión Parental
5) Violencia hacia la mujer

No obstante a todo lo anterior, y si bien existen tópicos transversales que tienen injerencia en ambas esferas de protección de datos personales, tanto de sujetos obligados como de particulares; existen temas que son propios de cada área, mismos que se desarrollarán a continuación.

5.3.2. Retos en materia de Datos Personales en el ámbito de los Sujetos Obligados

5.3.2.1. Desarrollo, implementación y ejecución de Programas Nacionales de Protección de Datos Personales

Actualmente el Programa Nacional de Protección de Datos Personales 2018-2022, (PRONADATOS), es un instrumento de política pública que atiende los elementos de una planeación estratégica adecuada para encauzar las acciones que en materia de protección de datos personales se desarrollen en el sector público a nivel nacional.

[426] El INAI habilitó un micrositio denominado “Guía para titulares de los datos personales”, el cual está compuesto por varias guías con el fin de cumplir con las obligaciones en materia de datos personales, el micrositio está disponible en: *https://home.inai.org.mx/?page_id=3402*

Este instrumento dispone de un cuadro que pretende reflejar las perspectivas presentes y futuras en el desarrollo y ejecución del PRONADATOS tal como se muestra a continuación:

Dónde estamos 2018- 2020 (etapa 1 PRONADATOS)	**Dónde estaremos** 2020-2022 (etapa 2 PRONADATOS)	**Hacia dónde vamos** 2022- 2026 (SEGUNDO PRONADATOS)	**Qué aspiramos** **2037** (20 años de la LGPDPPSO)
Se establecen las condiciones institucionales que permitan que los integrantes del SNT cumplan sus obligaciones establecidas en la LGPDPPSO y las legislaciones locales.	Los integrantes del SNT cumplen a cabalidad las obligaciones que les ha establecido la LGPDPPSO.	Los organismos garantes se consolidan como instituciones capaces de garantizar la protección de los datos personales de las y los titulares. Y los integrantes federales del SNT (AGN, ASF e INEGI) son parámetros de buenas prácticas en la materia.	El SNT se consolida como un mecanismo comprobado y reconocido para la generación de una garantía efectiva y homogénea del derecho a la protección de los datos personales para toda la población del país.
Se comienzan esfuerzos generalizados para incrementar el conocimiento del derecho y su ejercicio entre la población.	Hay un incremento en el porcentaje de personas que identifica la legislación en materia de protección de datos personales, así como en el conocimiento de las instituciones encargadas de la garantía de este derecho.	La población incrementa el ejercicio de su derecho a la protección de datos personales para proteger su privacidad y la de sus familiares.	La mayoría de la población identifica los mecanismos que le permiten ejercer su derecho a la protección de datos personales.
Se impulsa el cumplimiento de los responsables del ámbito público en los distintos niveles de gobierno en materia de sus obligaciones en materia de protección de datos personales.	Se evalúa a todos los responsables del ámbito público en el cumplimiento de sus obligaciones en materia de protección de datos personales.	Las instituciones públicas que manejan una mayor cantidad de datos personales lo hacen cumpliendo con lo dispuesto en la LGPDPPSO.	La gestión de la seguridad de la información en todos los niveles del sector público está internalizada y es aplicada constante y eficientemente por los servidores públicos.
Se generan líneas bases para la medición de los aspectos más relevantes de la protección de datos personales en el sector público.	Se desarrolla una serie de instrumentos y mecanismos que permiten contar con la información necesaria para la evaluación del estado que guardan los principales aspectos de la protección de datos en el sector público del país	Se cuenta con análisis de las fuentes de información que permiten dar cuenta de los cambios generados por las acciones del PRONADATOS	La generación de información, su conversión en conocimiento y su integración en la toma de decisiones en materia de protección de datos personales es una rutina institucionalizada en el Estado mexicano.

Imagen: Perspectivas del PRONADATOS.

Tomado de: SNT. *Programa Nacional de Protección de Datos Personales*, [en línea], DOF,26/01/2018 , [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://dof.gob.mx/nota_detalle.php?codigo=5511542&fecha=26/01/2018#gsc.tab=0.*

De las partes optimistas de ver este cuadro, destaca que tiene una visión al 2037, es decir a 20 años de la publicación de la LGPDPPSO, lo cual es positivo en tanto que ya existe una visión de Estado en esta materia de hacia dónde se quiere llegar; el problema, o mejor dicho, los problemas serán los que impidan que esta primer visión no se realice.

No es que sea un "ave de mal agüero"; sin embargo, considero que, si algo caracteriza al sector público, es su gran ineficiencia e ineficacia en el cumplimiento de metas programáticas por un sin número de claroscuros. Esto no significa que tampoco se haga nada, por supuesto que no, lo que significa es que las acciones y metas que se cumplen, serán menores en relación por lo que haga falta por cumplir.

Peor aún, cuando en este PRONADATOS en la parte de indicadores generales y transversales del Programa, se colocan los objetivos e indicadores por eje temático; pero en la gran mayoría no se colocan metas a cumplir, solo se indican "Por definir", veamos un ejemplo:

Educación y cultura de protección de datos personales entre la sociedad mexicana		
Objetivo	**Indicador**	**Meta**
Fomentar el conocimiento generalizado de la protección de los datos personales	Porcentaje de quejas por mal uso de datos personales presentadas ante instituciones públicas que reciben los Organismos Garantes ENAID	**Por definir**
Fomentar el conocimiento generalizado de la protección de los datos personales	Presupuesto asignado a cada Órgano Garante, para la implementación de Programas de Educación y Cultura de Protección de Datos Personales.	**Por definir**

Imagen: Metas por definir en materias de cultura de protección de datos personales.
Tomado de: SNT. *Programa Nacional de Protección de Datos Personales*, [en línea], DOF,26/01/2018 , [fecha de consulta: 5 de diciembre de 2022] Disponible en:
https://dof.gob.mx/nota_detalle.php?codigo=5511542&fecha=26/01/2018#gsc.tab=0.

De lo anterior, se puede apreciar que lamentablemente si no contamos con elementos de medición, finalmente no se podrían medir avances o formas de saber qué porcentajes faltaron por cumplir de cada uno de los elementos. Ya será el Consejo Consultivo el que determine, las metas a cumplir.

5.3.2.2. Errores en el tratamiento de datos personales por parte de los sujetos obligados

El actual PRONADATOS muestra en su diagnóstico, lo que podríamos considerar riesgos o "problemáticas" detectadas en el tratamiento de los datos, tal como se muestra a continuación:

Principales problemáticas detectadas		
Capacitación a los responsables en materia de protección de datos personales	Implementación y mantenimiento de un sistema de gestión de seguridad	Estándares nacionales, internacionales y buenas/mejores prácticas en la materia
▪ Se desconoce el universo de atención ▪ La LGPDPPSO ha definido nuevas y más amplias obligaciones y facultades para los responsables, las cuales desconocen ▪ Se carece de criterios para identificar necesidades, priorizaciones y sectorizaciones adecuados para atender las necesidades de capacitación en el sector público ▪ Las políticas de capacitación no están vinculadas a los programas sustantivos ▪ No existen las capacidades técnicas, entre los servidores públicos, en materia de protección de datos personales (profesionalización)	▪ Pueden darse vulneraciones de seguridad que afecten de manera significativa los derechos de los titulares ▪ Las medidas de seguridad y el tratamiento de datos ante las nuevas tecnologías de la información son desconocidos y carecen de un marco de certeza ▪ Hay un desconocimiento generalizado de las medidas de seguridad informática	▪ No han sido identificados los incentivos que permitan a los responsables adoptar mejores prácticas

Ante este diagnóstico, tenemos que plantearnos sobre todo la falta de profesionalización de los servidores públicos en los sujetos obligados. Tristemente, recién el titular del ejecutivo federal, mencionó datos personales de un reconocido periodista refiriéndose a sus ingresos derivados de personas privadas.

Este suceso, se puede considerar lamentable no solo por el tipo de persona, que aunque sea una persona pública, (Carlos Loret de Mola) es un ciudadano como cualquiera de nosotros, que por diferentes razones puede ser vulnerado en sus datos personales.

La rotación de los servidores públicos es otro problema que puede llevar a errores,

como se sabe, a la entrada de los “nuevos” equipos de trabajo, lo normal es que lleguen nuevas personas a ocupar diferentes cargos en las estructuras de los sujetos obligados, lo que puede llegar a generar tanto falta de personal en las áreas, como la falta de profesionalización a la que nos hemos referido líneas arriba.

Otros riesgos que a consideración del que esto escribe pueden derivar en errores durante el tratamiento de datos personales por parte de sujetos obligados son los siguientes:

1. Tratamiento de comunicaciones privadas de parte de los ministerios públicos.
    a. Datos personales en carpetas de investigación.
    b. Datos personales de adolescentes infractores.
    c. Manejo de fotografías de detenidos o presuntos responsables.
    d. Datos personales de las víctimas.
2. Derecho a la imagen y derechos de autor.
3. Tratamiento de imágenes y otro tipo de datos personales de menores de edad.
4. Datos personales implicados en prácticas monopólicas.
5. Tratamiento de datos personales de partes en asuntos de conocimiento de los órganos del Poder Judicial de la Federación.
6. Límites en el derecho a la información cuando impliquen datos personales.
7. Conocimiento público de Datos personales cuando se presenten determinaciones fiscales, aduanales o de seguridad social.
8. Datos personales e información confidencial.
9. Publicaciones en páginas oficiales de internet, o redes sociales oficiales o de servidores públicos.
10. Sistemas de protección de datos personales, sistemas archivísticos y de transparencia y acceso a la información pública, así como en el caso de rendición de cuentas.
11. Supresión de Datos Personales.
12. Datos personales y la desclasificación de la información.
13. Datos personales en materia electoral.
14. Manejo del tratamiento de datos personales del Registro Público de Usuarios.
15. Datos personales en expedientes clínicos.
16. Datos personales difundidos por sujetos obligados.
17. Versiones públicas y datos personales.

Muchos de estos riesgos de alguna manera, ya han sido interpretados mediante criterios emitidos por el Poder Judicial de la Federación, pero en varios de ellos apenas son tesis aisladas, lo que significa que aún falta mucho camino que recorrer.

5.3.2.3. Evolución de corpus iuris en datos personales

El proyecto *Corpus Iuris* en materia de protección de datos personales es un proyecto que surge en el seno de la Red Iberoamericana de Protección de Datos, con el objetivo de contar con una herramienta que permita acceder de manera sencilla y sistematizada a un nutrido conjunto de documentos, normas y

precedentes que muestren el desarrollo que ha tenido la protección de datos personales como un derecho humano, las direcciones y grados de avance que éste ha alcanzado, así como las áreas que es necesario reforzar, continuar desarrollando, o bien, que representan nuevos retos en la materia.[427]

Los objetivos y la organización de la Red están recogidos en el Reglamento aprobado con motivo del VI Encuentro Iberoamericano de Protección de Datos (EIPD), celebrado en mayo de 2008, y revisado en el XVI EIPD, en noviembre de 2018, en San José, Costa Rica.

Asimismo, la estrategia de la Red Iberoamericana de Protección de Datos para el periodo 2021-2025 estará orientada al desarrollo de los siguientes objetivos e iniciativas:[428]

1. Marco regulatorio de convergencia regional.
2. Espacio que promueva la cooperación efectiva entre las Autoridades Iberoamericanas de Protección de Datos.
3. Institucionalización y profesionalización de las Autoridades como factor esencial para reforzar su estabilidad e independencia.
4. Investigaciones frente a casos que impactan a titulares de datos de países de la Red.
5. Red con proyección de liderazgo en el escenario internacional.
6. Nuevos escenarios para la protección de datos: innovación, protección de datos y responsabilidad social (sostenibilidad)
7. Mayor presencia de la protección de datos en el ámbito judicial.
8. Red abierta a las organizaciones sociales y a otros actores de la sociedad civil.
9. Red que refuerce las relaciones con los profesionales de la privacidad y sus organizaciones.
10. Red que promueva la relaciones con el mundo académico y docente.
11. Red que refuerce la relaciones con el sector público.
12. Red que promueva la relaciones con el sector empresarial.

5.3.2.3. Tecnologías de la Información en datos personales para sujetos obligados

Vivimos actualmente en un mundo donde “gracias” a esta emergencia sanitaria, el uso de las TIC´s se volvieron cada vez más y más usuales.

Hoy en días podemos hablar de la *smartificación* y robotización de la administración pública. “Por *smartificar* en el ámbito público se entiende el uso global, intensivo y

[427] INAI, *Corpus Iuris Internacional y Nacional*, [en línea], México, INAI, s.a., [fecha de consulta: 5 de diciembre de 2022] Disponible en: *http://corpusiurispdp.inai.org.mx/Pages/home.aspx*
[428] Red Iberoamericana de Protección de Datos, *Plan Estratégico 2021-2025 red Iberoamericana de Protección de Datos (RIPD)*, [en línea] España, RIPD, 2020, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://www.redipd.org/sites/default/files/2020-12/Plan-Estrategico-RIPD-2021-2025.pdf* pp. 3-10.

sostenible de las tecnologías de la información bajo el principio de servicio para la mejora de calidad de los ciudadanos".[429]

La *smartificación* de la Administración pública implica actualmente la utilización del *big data* con tres objetivos básicos:[430]

a) Mejorar la calidad de los servicios a los ciudadanos;
b) Mejorar la inteligencia institucional para incrementar la capacidad en la toma de decisiones, de control y evaluación de las políticas públicas; y
c) Mejorar la inteligencia institucional para lograr mayor capacidad para ejercer el papel de dirección de las complejas redes de gobernanza públicas-públicas (administración nuclear versus administración instrumental: organismos autónomos, empresas públicas, consorcios y fundaciones) y públicas-privadas (colaboración con organizaciones privadas con o sin ánimo de lucro).

5.3.3. Retos en materia de Datos Personales en Posesión de Particulares

5.3.3.1. Influencia de la Inteligencia Artificial, para la toma de decisiones utilizando el Big Data

La Inteligencia Artificial o IA "es la capacidad de las máquinas para usar algoritmos, aprender de los datos y utilizar lo aprendido en la toma de decisiones tal y como lo haría un ser humano. Sin embargo, a diferencia de las personas, los dispositivos basados en IA no necesitan descansar y pueden analizar grandes volúmenes de información a la vez."[431]

Al ir evolucionando la IA, estas han comenzado a desarrollar habilidades artificiales como "ver (visión artificial), oír, (reconocimiento de voz), y entender (procesamiento del lenguaje natural)",[432] tal como se aprecia en la siguiente figura:

[429] Ramió, Carles, *Inteligencia artificial y administración pública. Robots y humanos compartiendo el servicio público*, España, Catarata, 2019, p. 8.
[430] *Ídem*.
[431] Petteri Rouhiainen, Lasse, *Inteligencia Artificial, 101 cosas que debes saber hoy sobre nuestro futuro*, [en línea], España, Planeta, 2018, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://www.planetadelibros.com/libros_contenido_extra/40/39307_Inteligencia_artificial.pdf* p. 17.
[432] *Ibidem*, p. 23.

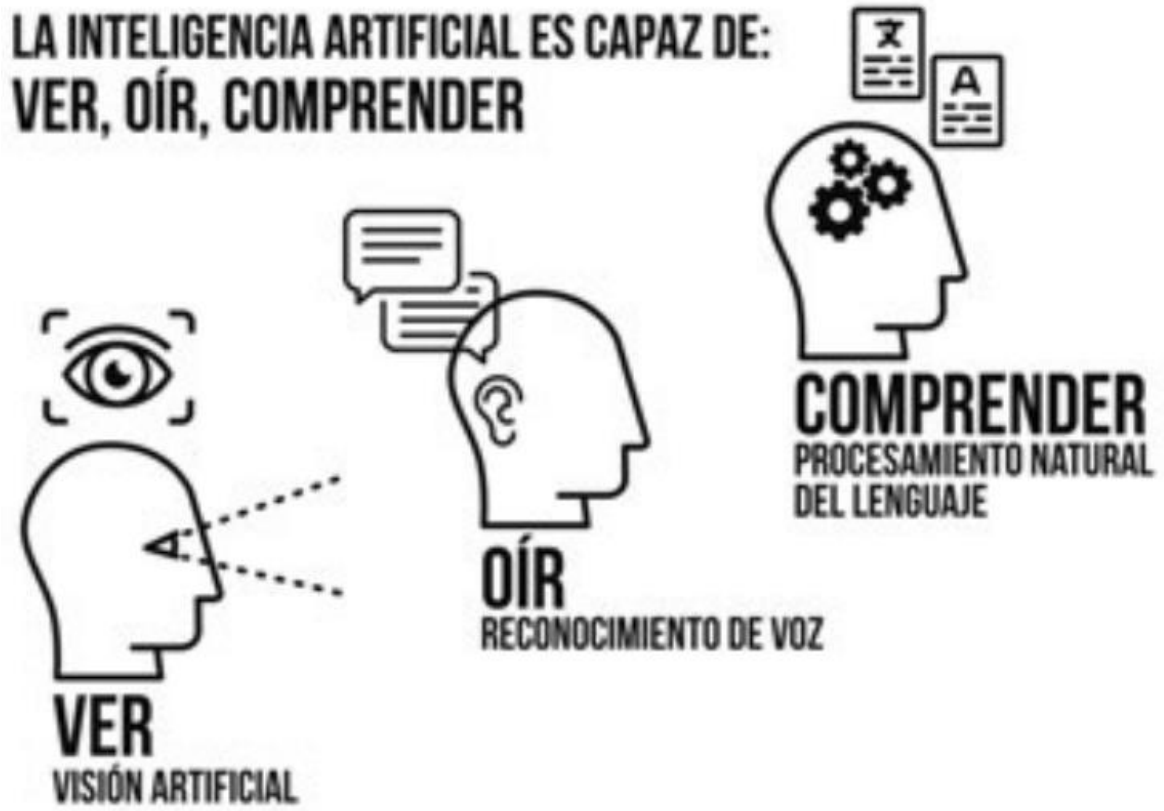


Imagen: Capacidades de la inteligencia artificial (IA).
Tomado de: Petteri Rouhiainen, Lasse, *Inteligencia Artificial, 101 cosas que debes saber hoy sobre nuestro futuro*, [en línea], España, Planeta, 2018, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://www.planetadelibros.com/libros_contenido_extra/40/39307_Inteligencia_artificial.pdf* p. 23.

Gracias a los macro volúmenes de información que se generan y procesan cada día por medio de ordenadores cada vez más y más potentes, la IA se ha acelerado, teniendo aplicaciones de reconocimiento de biométricos, textos, telemedicina y toma de decisiones.

Bernardo Pérez Orozco manifiesta como aplicaciones de la IA las siguientes:[433]

- **Reconocimiento visual**: sistemas capaces de reconocer y rastrear objetos y personas en imágenes y video.
- **Reconocimiento del lenguaje natural**: sistemas capaces de reconocer, reproducir de modo artificial y descifrar el significado del lenguaje hablado. Incluye también la traducción automática entre diferentes idiomas, así como respuestas automáticas de preguntas y el análisis y síntesis de documentos.
- **Estrategia y planeación**: sistemas capaces de generar estrategias optimizadas para resolver problemas de gran complejidad y a largo plazo. Algunos ejemplos son los sistemas autómatas, capaces de apoyar en tareas

[433] Pérez Orozco, Bernardo*, Inteligencia artificial*, [en línea] México, Nota-INCyTU, Número 012, Marzo 2018, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://www.foroconsultivo.org.mx/INCyTU/documentos/Completa/INCYTU_18-012.pdf* p. 2.

de logística y manufactura, jugar videojuegos o navegar a través de espacios físicos.

- **Diagnóstico y apoyo en la toma de decisiones**: sistemas capaces de analizar problemas complejos y ayudar a tomar decisiones, por ejemplo, en medicina, en la detección de enfermedades o la elección del tratamiento más adecuado. Incluye también el análisis de datos para agilizar el desarrollo de medicamentos.
- **Colaboración humano-computadora**: Consiste en incorporar sistemas inteligentes como parte de equipos de trabajo humanos. Por ejemplo, para responder más ágilmente a desastres naturales, se han desarrollado sistemas que pueden analizar vistas aéreas de las zonas afectadas para identificar dónde se requiere mayor apoyo.

Las regulaciones legales apenas son incipientes: Por ejemplo, el Reglamento Europeo de Protección de Datos en su artículo 22 dispone lo siguiente:

> Artículo 22
> Decisiones individuales automatizadas, incluida la elaboración de perfiles
> 1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

Por su parte, la Red Iberoamericana de Protección de Datos (RIPD) ha elaborado un documento intitulado: "Recomendaciones generales para el tratamiento de datos en la inteligencia artificial", cuyo objetivo es presentar algunas sugerencias a quienes desarrollan productos de IA, con el fin de orientarlos para que desde el diseño del producto se tengan en cuenta las exigencias de las regulaciones sobre tratamiento de datos personales. Por lo tanto, las mismas solo son aplicables a ese tipo de información –datos personales- y no a cualquier información en general.

Estas recomendaciones tienen un enfoque preventivo y parten del supuesto según el cual la mejor forma de proteger los derechos humanos comprometidos en el tratamiento de datos personales es evitando su vulneración.

Para conocer los detalles de la implementación de algunas de estas recomendaciones, la RIPD ha elaborado unas directrices complementarias y más detalladas contenidas en el documento denominado "Orientaciones específicas para el cumplimiento de los principios y derechos que rigen la protección de los datos personales en los proyectos de Inteligencia Artificial".[434]
Por lo anterior, la RIPD ha recomendado la Gestión de Riesgos de algoritmos de la

[434] Red Iberoamericana de Protección de Datos, *La RIPD aprueba sendos documentos sobre Inteligencia Artificial y Protección de Datos Personales*, [en línea] España, RIPD, 19 de febrero de 2020, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://www.redipd.org/es/noticias/la-ripd-aprueba-sendos-documentos-sobre-inteligencia-artificial-y-proteccion-de-datos*

siguiente manera:[435]

Imagen: Gestión de riesgos de los algoritmos.
Tomado de: Red Iberoamericana de Protección de Datos, *Recomendaciones Generales para el tratamiento de Datos en la Inteligencia Artificial*, [en línea] RIPD, México, 2019, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://www.redipd.org/sites/default/files/2020-02/guia-recomendaciones-generales-tratamiento-datos-ia.pdf* p. 18.

5.3.3.2. Derecho al Olvido

Este es uno de los sub derechos de protección de datos personales, más controversiales que se debaten actualmente, más ahora que tenemos una huella digital que se podría decir que nos persigue dondequiera que vayamos. Hoy hablamos también de identidad digital, reputación digital, branding personal y un sinfín de términos que se pueden asociar a la persona en el entorno digital.

Iniciemos con dos definiciones del Diccionario de la Real Academia Española:

[435] Red Iberoamericana de Protección de Datos, *Recomendaciones Generales para el tratamiento de Datos en la Inteligencia Artificial*, [en línea] RIPD, México, 2019, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://www.redipd.org/sites/default/files/2020-02/guia-recomendaciones-generales-tratamiento-datos-ia.pdf* p. 18.

Olvido[436]	**Olvidar**[437]
De olvidar. 1. m. Cesación de la memoria que se tenía. 2. m. Cesación del afecto que se tenía. 3. m. Descuido de algo que se debía tener presente. dar, o echar, al olvido, o en olvido 1. locs. verbs. olvidar (‖ dejar de retener en la mente). enterrar en el olvido 1. loc. verb. Olvidar para siempre.	Del lat. vulg. **oblitāre*, y este der. del lat. *oblītus*, part. de *oblivisci*. 2. tr. Dejar de tener en cuenta algo. Olvida lo dicho. 5. tr. Dejar de tener afecto o estima por alguien o algo. Me olvidaste muy pronto. 6. tr. desus. Hacer perder la memoria de algo. 7. prnl. Perder de la memoria, de la consideración o de la estima. Se olvidó DE mi teléfono. Se olvidan DE un detalle. Me olvidé DE avisarte. Nunca se olvidó DE ella. olvídate, o que te olvides, que se olvide, etc. 1. exprs. coloqs. U. para indicar a alguien que debe perder toda esperanza de algo.

Enfocándonos desde la óptica jurídica, el derecho al olvido se le conoce de diferentes formas como: Derecho al olvido, derecho al olvido digital, derecho al olvido en Internet, derecho al olvido en la red, derecho de supresión, derecho a la desindexación, derecho a la oscuridad digital, *right to be forgotten, right to delete, right to erasure, right to be delisted*, y *right to oblivion*.[438]

Trasladando esta definición gramatical al mundo jurídico, los conceptos parecen no estar tan claros; e incluyen diferentes directrices. Por ejemplo, la Agencia Española de Protección de Datos define el derecho al olvido de la siguiente forma:

[436] OLVIDO: Real Academia Española, *Diccionario de la Real Academia Española. Edición del Tricentenario*, [en línea] España, RAE, s.a. [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://dle.rae.es/olvido*

[437] OLVIDAR: Real Academia Española, *Diccionario de la Real Academia Española. Edición del Tricentenario*, [en línea] España, RAE, s.a. [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://dle.rae.es/olvidar*

[438] Guerrero Santillán, Elvia Celina, *El Derecho al olvido digital en México*, [en línea] México, Revista "Caja de cristal" ITEI-UDGVirtual, Año 4, No. 7, Ene-Jun 2018, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *http://www.itei.org.mx/v3/micrositios/revista_caja_cristal/numeros/num7_CDC_julio2018.pdf* p. 57.

> Es la manifestación del derecho de supresión aplicado a los buscadores de internet. El derecho de supresión ('derecho al olvido') hace referencia al derecho a impedir la difusión de información personal a través de internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa. En concreto, incluye el derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público, aunque la publicación original sea legítima (en el caso de boletines oficiales o informaciones amparadas por las libertades de expresión o de información).[439]

Elvia Celina Guerrero, menciona que existen diversas interpretaciones de lo que se denomina derecho al olvido digital y nos proporciona diferentes interpretaciones del mismo:[440]

a) Una forma de manifestación del derecho de autodeterminación informativa (Murillo, 1993).
b) Un interés jurídicamente protegido (Álvarez, 2015).
c) Una forma de caducidad del dato negativo (Puccinelli, 2012)
d) La aplicación de derechos ya existentes en relación a la protección de datos (Castellano, 2015 y Dulong y Guadamuz, 2016).
e) La posibilidad de borrar información personal de Internet (Bennet 2012 y Valderrama, 2016).
f) La facultad de solicitar la supresión de datos personales en Internet (Reglamento del Parlamento Europeo y del Consejo de 27 de abril de 2016).
g) La facultad de solicitar la supresión de los enlaces a páginas de Internet que contengan datos personales (Pazos, 2015).
h) La posibilidad de que no aparezcan las páginas con información personal en los resultados de las búsquedas de información en Internet (Consejo Asesor de Google, 2015).

Ahora bien, la Dra. Isabel Davara sostiene que el este concepto está fundado sobre "instituciones jurídicas previas, como son la prescripción de delitos, la eliminación de antecedentes penales o las amnistías en temas financieros y fiscales."[441] En este sentido el derecho al olvido estaría amparado, "por su semejanza, con el derecho a la cancelación o, en su caso, con derecho de oposición, derechos dentro de los denominados ARCO."[442]

---

[439] Agencia Española de Protección de Datos, *Derecho de supresión ("al olvido"): buscadores de internet*, [en línea], España, AEPD, 2021, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://www.aepd.es/es/areas-de-actuacion/internet-y-redes-sociales/derecho-al-olvido*
[440] Guerrero Santillán, Elvia Celina, *op. cit*. p.57.
[441] Davara Fernández de Marcos, Isabel, *El derecho al olvido en relación con el derecho a la protección de datos personales*, [en línea] México, INFODF (HOY INFOCDMX) Ensayos, No. 23, 2014, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://infocdmx.org.mx/capacitacion/publicacionesDCCT/ensayo23/23ensayo2014.pdf* p. 34.
[442] *Ídem.*

El caso más emblemático se tiene en Europa de fecha 13 de mayo de 2014 relativo a la sentencia del Tribunal de Justicia europeo en el procedimiento entre Google Spain, S.L, Google INC., contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González.

Las conclusiones de esta sentencia refieren lo siguiente:[443]

1) La actividad de un motor de búsqueda, que consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia determinado, debe calificarse de «tratamiento de datos personales», cuando esa información contiene datos personales, y, por otro, el gestor de un motor de búsqueda debe considerarse «responsable» de dicho tratamiento.
2) Se lleva a cabo un tratamiento de datos personales en el marco de las actividades de un establecimiento del responsable de dicho tratamiento en territorio de un Estado miembro, en el sentido de dicha disposición, cuando el gestor de un motor de búsqueda crea en el Estado miembro una sucursal o una filial destinada a garantizar la promoción y la venta de espacios publicitarios propuestos por el mencionado motor y cuya actividad se dirige a los habitantes de este Estado miembro.
3) El gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de estas páginas web, y, en su caso, aunque la publicación en dichas páginas sea en sí misma lícita.
4) Se tendrá que examinar, en particular, si el interesado tiene derecho a que la información en cuestión relativa a su persona ya no esté, en la situación actual, vinculada a su nombre por una lista de resultados obtenida tras una búsqueda efectuada a partir de su nombre, sin que la apreciación de la existencia de tal derecho presuponga que la inclusión de la información en cuestión en la lista de resultados cause un perjuicio al interesado. Puesto que éste puede, solicitar que la información de que se trate ya no se ponga a disposición del público en general mediante su inclusión en tal lista de resultados, estos derechos prevalecen, en principio, no sólo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en acceder a la mencionada información en una búsqueda que verse sobre el nombre de esa persona. Sin embargo, tal no sería el caso si resultara, por razones concretas, como el papel desempeñado por el interesado en la vida pública, que la injerencia en sus derechos

[443] Tribunal de Justicia de la Unión Europea, *Sentencia caso Google vs AEPD y otro*, [en línea] España, InfoCuria, 13 de mayo de 2014, Asunto C-131/12, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES*

fundamentales está justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información de que se trate.

Derivado de esta sentencia los buscadores mayoritarios han habilitado formularios propios para recibir las peticiones de ejercicio del derecho de supresión, dichas plataformas son Google, Bing y Yahoo.
Para fines ilustrativos se mostrarán algunos aspectos del formulario para solicitar la retirada de información personal de Google, con base en el Reglamento General de Protección de Datos de Europa:[444]

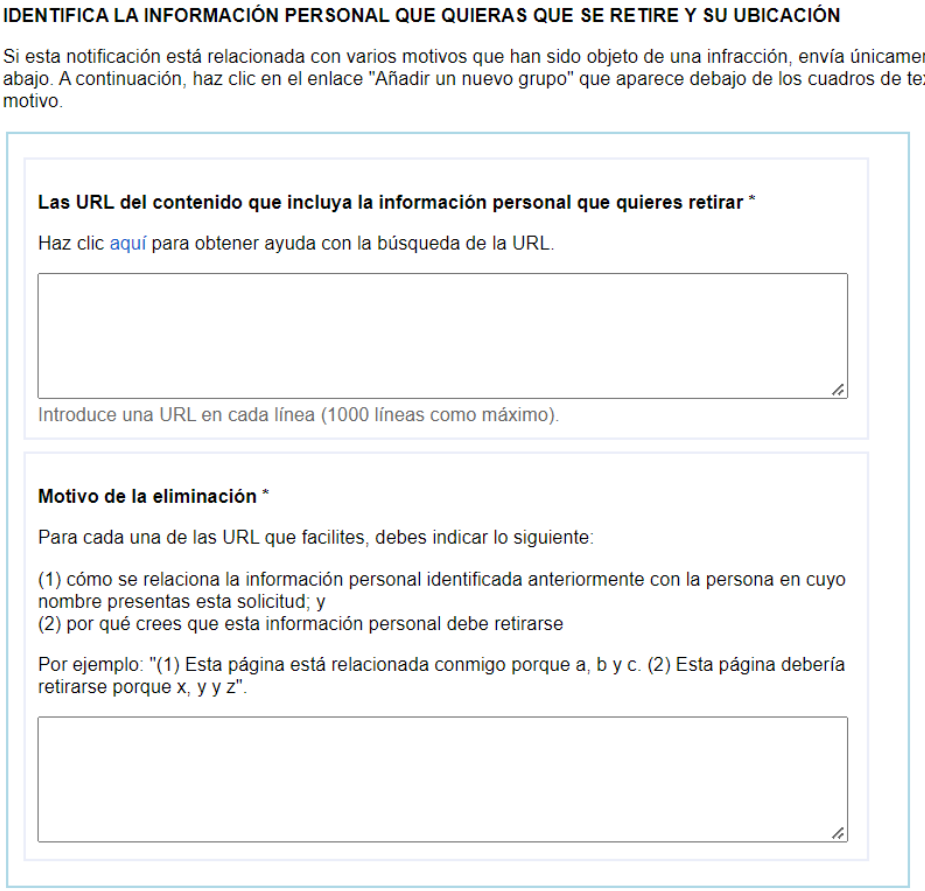


Imagen: Formulario de solicitud de retirada de datos personales I.
Tomado de: Google, *Formulario para solicitar la retirada de información personal*, [en línea] s.d., [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=637820066504967017-4005424&hl=es&rd=1*

[444] Google, *Formulario para solicitar la retirada de información personal*, [en línea] s.d., [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=637820066504967017-4005424&hl=es&rd=1*

Nombre utilizado para realizar búsquedas *

Este debería ser el nombre que, si se utiliza como consulta de búsqueda, produzca los resultados que quieres eliminar del registro. Si quieres enviar varios nombres (por ejemplo, si tu apellido de soltera es diferente al que utilizas ahora), utiliza una barra diagonal ("/") para separarlos. Por ejemplo, "Ana García / Ana Díaz".

DECLARACIONES JURADAS

Lee las siguientes afirmaciones y marca sus casillas para confirmar que las has leído y las aceptas.

☐ He leído y confirmo que he entendido la explicación del tratamiento de la información personal que envío, como se describe a continuación: *

Google LLC utilizará la información personal que facilites en este formulario (como tu dirección de correo electrónico y todos los datos de identificación) y la información personal que envíes en otros mensajes para procesar tu solicitud y cumplir con nuestras obligaciones legales. Google puede compartir información de tu solicitud con las autoridades de protección de datos, pero solo si la solicitan para investigar o revisar una decisión que Google haya tomado. Esto suele ocurrir si te has puesto en contacto con la autoridad de protección de datos nacional en relación con nuestra decisión. Si, debido a tu solicitud, se han retirado URLs de nuestros resultados de búsqueda, Google puede facilitar información a los webmasters de dichas URL.

Ten en cuenta que si has iniciado sesión en tu cuenta de Google, podemos asociar tu solicitud a esa cuenta.

☐ Declaro que la información de esta solicitud es precisa y que estoy autorizado para enviarla. *

☐ Comprendo que Google LLC no podrá procesar mi solicitud si el formulario no se ha rellenado correctamente o si la solicitud está incompleta. *

FIRMA

Fecha de la firma: *

MM/DD/YYYY (por ejemplo, "12/19/2010")

Firma: *

por ejemplo, Juan Pérez

Imagen: Formulario de solicitud de retirada de datos personales II.
Tomado de: Google, *Formulario para solicitar la retirada de información personal*, [en línea] s.d., [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=637820066504967017-4005424&hl=es&rd=1*

Adicionalmente, en la Unión Europea se creó un Grupo de Trabajo de Protección de Datos Artículo 29 el cual emitió las Directrices sobre la ejecución de la sentencia del Tribunal de Justicia de la Unión Europea de fecha 26 de noviembre de 2014, el cual está basado en dos partes:[445]

[445] Comisión Europea, *Directrices sobre la ejecución de la sentencia del tribunal de justicia de la unión europea en el asunto «google spain and inc contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González» c-131/12*. [en línea], 2014, s.d., [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A62012CJ0131*

Parte I: Interpretación de la sentencia del TJUE	Parte II: Lista de criterios comunes para la gestión de las reclamaciones por parte de las autoridades europeas de protección de datos
A. Los motores de búsqueda como responsables del tratamiento y su legitimación B. Ejercicio de los derechos C. Ámbito de aplicación D. Comunicación a terceros E. Función de las Autoridades de Protección de Datos	1. ¿Se refiere el resultado de la búsqueda a una persona física? ¿Es el resultado de la búsqueda consecuencia de una búsqueda realizada a partir del nombre del interesado? 2. ¿Desempeña el interesado un papel en la vida pública? ¿Es el interesado un personaje público? 3. ¿Es el interesado menor de edad? 4. ¿Son exactos los datos? 5. ¿Son los datos relevantes y no excesivos? a. ¿Se refieren los datos a la vida laboral del interesado? b. ¿Remite el resultado de la búsqueda a información supuestamente constitutiva de un delito de incitación al odio, calumnia, difamación u otros delitos similares de expresión contra el reclamante? c. ¿Reflejan los datos de forma evidente la opinión personal de alguien, o parece tratarse de hechos verificados? 6. ¿Se trata de información sensible, con arreglo a lo dispuesto en el artículo 8 de la Directiva 95/46/CE? 7. ¿Están actualizados los datos? ¿Están disponibles los datos desde hace más tiempo del necesario para cumplir el fin que se perseguía con su tratamiento? 8. ¿Causa perjuicio al interesado el tratamiento de los datos? ¿Tienen los datos un impacto desproporcionadamente negativo en el interesado? 9. ¿Remite el resultado de la búsqueda a información que pone en riesgo al interesado? 10. ¿En qué contexto se ha publicado la información? a. ¿Ha sido hecho público el contenido voluntariamente por el interesado? b. ¿Va dirigido el contenido a hacerse público? ¿Hay motivos razonables para entender que el interesado sabía que el contenido iba a hacerse público? 11. ¿Se publicó el contenido original con fines periodísticos?

	12. ¿Está facultado u obligado el editor de los datos a poner a disposición del público los datos personales? 13. ¿Hacen referencia los datos a un delito?

En México el caso más icónico lo tenemos en el Expediente PPD.0094/14 del entonces IFAI por un derecho de cancelación y oposición de datos personales ante Google México, S de R.L de C.V.[446] En dicho expediente, el entonces IFAI retoma diversos argumentos del expediente C-131/12 del tribunal de Justicia Europeo (citado arriba) y de lo cual el IFAI desprende que:

> {…] el prestador de un servicio de un motor de búsqueda en Internet es responsable del tratamiento que aplique a los datos de carácter persona que aparecen en las páginas web publicadas por terceros, por lo que bajo determinadas condiciones, cunado a raíz de una búsqueda efectuada a partir del nombre de una persona, la lista de resultados ofrezca enlaces a páginas web que contienen información sobre esa persona, ésta puede dirigirse directamente al gestor del motor de búsqueda para que se eliminen esos enlaces de la lista de resultados.
>
> Máxime si se considera que dicho tratamiento permite que cualquier internauta que utilice el motor de búsqueda para localizar información de una persona, a través de su nombre, tenga acceso a información sobre la vida de ésta de forma estructurada, de tal suerte que dicha circunstancia puede afectar los derechos humanos a la vida privada y a la protección de los datos personales."

En este procedimiento se ordenó a Google México a llevar a cabo las acciones necesarias a efecto de hacer efectivos de manera indubitable los derechos de oposición y cancelación objeto de protección en los siguientes términos:

1. Por lo que respecta al derecho de oposición, con fundamento en el artículo 27 de la Ley de la materia, se abstenga de tratar los datos personales del Titular, consistentes en su nombre y apellidos, de tal manera que al ser *tecleados* en el motor de búsqueda del Responsable, no aparezcan los links o URL2S – indexación- que dicho Titular refirió en su solicitud, […]
2. En cuanto al derecho de cancelación, con fundamento en los artículos 25 primer párrafo, de la LFPDPPP, y 106, 107 y 108 de su Reglamento, cancele los datos personales del Titular antes mencionados, de modo que no obren en las bases de datos del Responsable.

Tal fue la importancia de esta resolución que el 27 de enero de 2015, a través de la nota IFAI-OA/009/15 anunció que:

[446] s.d. *Resolución INAI*, *Google, Expediente: PPD.0094/14* [en línea] México, s.a., [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2017/06/Mexico-RTBF-INAI-DerechoOlvidoCorrupcion.pdf*

> En un hecho sin precedente, el Pleno del Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) inició un procedimiento de imposición de sanciones en contra de Google México, S. de R.L. de C.V., filial del gigante de las redes sociales, por posibles infracciones a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).
>
> Además, ordenó a dicha empresa hacer efectivos los derechos de cancelación y oposición al tratamiento de los datos personales de un particular.[447]

Esta resolución fue impugnada, donde el Juzgado Decimoquinto de Distrito en Materia Administrativa de la Ciudad de México niega el amparo. Fortuna pide la revisión de la sentencia. El caso se asigna al Séptimo Tribunal Colegiado de Circuito del Centro Auxiliar de la Primera Región (expediente auxiliar 355/2016). Para agosto de 2016, se concede el amparo por falta al debido proceso (violación a su derecho de audiencia). La resolución del INAI queda sin efecto, por lo que no se pudo resolver el fondo del asunto.[448]

En diciembre de 2019, el grupo parlamentario de Morena por conducto del Senador Ricardo Monreal presentó una iniciativa de reforma a la LFPDPPP en materia de "Derecho de Olvido". Dicha iniciativa mencionaba que:

> […] en México se encuentran reconocidos los derechos A.R.C.O; es precisamente el derecho de cancelación el que ocupa el interés de esta iniciativa puesto que, lo que se conoce como derecho al olvido es una extensión del derecho de cancelación, cuyo ámbito de aplicación se traslada a los datos personales que se hallen digitalizados y en tal sentido disponibles para su acceso y consulta en los motores de búsqueda de internet, las plataformas digitales y los demás medios que hacen parte del mundo digital.[449]

Dentro de las modificaciones propuestas destaca la ampliación de un tipo de datos personales denominados Datos personales digitalizados, lo cual se propuso en los siguientes términos:

---

[447] INAI, *En un hecho sin precedente, el IFAI inició un procedimiento de imposición de sanciones en contra de Google México*, [en línea], México, INAI, Nota IFAI-OA/009/15, 27 de enero de 2015, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *http://inicio.inai.org.mx/Comunicados/Comunicado%20IFAI-009-15.pdf* p. 1.

[448] Soto Galindo, José, *Fortuna obliga al INAI a discutir sobre Google y los datos personales otra vez*, [en línea] México, Revista El Economista, Secc. Opinión, 25 de agosto de 2016, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://www.eleconomista.com.mx/opinion/Fortuna-obliga-al-INAI-a-discutir-sobre-Google-y-los-datos-personales-otra-vez-20160825-0002.html*

[449] ´Monreal Ávila, Ricardo, *Iniciativa con proyecto de decreto que reforma, adiciona y modifica diversas disposiciones de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, en materia de Derecho de* Olvido, [en línea] México, Senado de la República, Grupo Parlamentario de Morena, LXIV Legislatura, 03 de diciembre de 2019, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://infosen.senado.gob.mx/sgsp/gaceta/64/2/2019-12-03-1/assets/documentos/Inic_Morena_Sen_Monreal_Posesion_Particulares.pdf* p. 6.

> Artículo 3.- Para los efectos de esta Ley, se entenderá por:
> VI Bis. Datos personales digitalizados: aquellos datos personales que se encuentran en medios electrónicos, plataformas digitales, buscadores de internet y demás medios digitales, incluyendo textos, comentarios, interacciones, ubicaciones, contenido multimedia, antecedentes penales cuando la condena haya sido cumplido o el delito hubiere prescrito, y demás información.

La parte central del Derecho al Olvido quedó plasmada en la propuesta de añadir un párrafo al artículo 25 de la LFPDPPP en la parte de derecho de cancelación, lo cual se propuso en los siguientes términos:

> Artículo 25.- El titular tendrá en todo momento el derecho a cancelar sus datos personales.
> …
> **Tratándose de datos personales digitalizados, el derecho de cancelación abarcará la eliminación y supresión de todos los contenidos que se encuentren en medios electrónicos, plataformas digitales, buscadores de internet y demás medios digitales, incluyendo textos, comentarios, interacciones, ubicaciones, contenido multimedia, antecedentes penales y demás información.**

Asimismo, dicha propuesta busca añadir un artículo 26 bis, relacionado con la procedencia de la cancelación de datos personales digitalizados, de la siguiente manera:

> Artículo 26 Bis. Para que proceda la cancelación de los datos personales digitalizados deberá configurarse, al menos, una de las circunstancias siguientes:
> a) que la información sea innecesaria en relación con los fines para los cuales fue recogida o proporcionada;
> b) que los datos personales digitalizados hayan sido tratados ilícitamente;
> c) que la información sea inexacta, y
> d) que la información sea obsoleta o irrelevante.
> En todo caso, la ampliación del derecho a la cancelación de los datos personales digitalizados no podrá ejercerse cuando su ejercicio vulnere la seguridad nacional y el orden público.

Cabe señalar que esta iniciativa no recibió el dictamen y pasó al “olvido” el 18 de noviembre de 2021.[450]

Por último, el pasado 04 de agosto de 2021, se publicaron en la Gaceta Oficial de la Ciudad de México, diversas modificaciones al Código Civil relacionadas con aspectos digitales, entre ellos, se añadió el artículo 1392 Bis, que refiere a la parte del Derecho al Olvido en los siguientes términos:

[450] Cámara de Senadores, *Gaceta del Senado*, [en línea] México, GACETA: LXIV/2PPO-67/102681, jueves 05 de diciembre de 2019, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://www.senado.gob.mx/64/gaceta_del_senado/documento/102681*

Artículo 1392 Bis. El legado también puede consistir en la titularidad sobre bienes o derechos digitales almacenados en algún equipo de cómputo, servidor, plataforma de resguardo digital, dispositivo electrónico, redes sociales o dispositivos físicos utilizados para acceder a un recurso restringido electrónicamente, los cuales pueden consistir en:
I. Cuentas de correo electrónico, sitios, dominios y direcciones electrónicas de internet, archivos electrónicos tales como imágenes, fotografías, videos, textos; y

II. Claves y contraseñas de cuentas bancarias o de valores, aplicaciones de empresas de tecnología financiera de los que el testador sea titular o usuario y para cuyo acceso se requiera de un nombre o clave de usuario, clave y contraseña.

Los bienes o derechos digitales serán independientes de su valor económico y contenido determinable.

Los datos necesarios para el acceso a los bienes o derechos digitales podrán ser resguardados por el mismo notario en el apéndice del instrumento correspondiente al testamento o en el caso de la actuación digital notarial a que se refiere la Ley del Notariado para la Ciudad de México, en un sistema de almacenamiento permanente.

El testador podrá nombrar a un ejecutor especial que, constatado que se trató del último testamento otorgado y su validez fue reconocida, estará facultado para que se le proporcione la información correspondiente a los accesos de los bienes o derechos digitales y proceda según las indicaciones del testador.

La gestión de la información a que se refiere el primer párrafo de este artículo no implicará que el ejecutor especial sea titular de dichos bienes o derechos digitales o que pueda disponer de ellos, salvo disposición del testador.

Si el testador no dispuso sobre el tratamiento de su información personal almacenada en registros electrónicos públicos y privados, incluyendo imágenes, audio, video, redes sociales y cualquier método de búsqueda de internet o, en su caso, ordenó su eliminación, una vez que se tenga certeza de que se trata del último testamento y se haya declarado la validez del mismo, el albacea o el ejecutor especial procederá de inmediato a solicitar su eliminación a las instituciones públicas y/o privadas que conserven dicha información a fin de salvaguardar el ***derecho al olvido*** a favor del autor de la sucesión, salvo disposición expresa de éste.

Parece que ni en la muerte se puede estar en paz. El derecho al olvido, tiene connotaciones que van desde el derecho a la intimidad y el derecho al honor; aunque, por otra parte, también podría ser un cierto tipo de ataque contra la libertad de expresión y la libertad de dar a conocer asuntos que son de interés público, en

algo que se conoce como el derecho a la verdad.

De tal manera que el derecho al olvido es una especie de “arma” de doble filo, entre nuestra capacidad de elegir sobre qué tipo de información de nosotros queremos que se quedé en la red, y la opacidad o abuso en esta figura.

De cualquier formar los buscadores mexicanos podrían adoptar el ejemplo de los buscadores mexicanos podrían generar procedimientos ad-hoc, para desindexar la información relacionada con datos personales, sin alterar la parte de acceso a la información; es decir, que los motores de búsqueda deberán analizar las intenciones de la supresión de la información ponderando entre el perjuicio a la imagen del titular de la información o el ocultamiento de información con otros fines no lícitos.

Con el fin de cumplir con el derecho al olvido, la Agencia Española de Protección de Datos propone como parte de los riesgos de datos personales un listado de cumplimiento en los siguientes términos:[451]

LISTADO DE CUMPLIMIENTO	CUMPLE SI/NO
DERECHOS DEL INTERESADO. DERECHOS DE SUPRESIÓN («EL DERECHO AL OLVIDO»)	
Se suprimen los datos cuando no son necesarios en relación con los fines para los que fueron recogidos	
Se suprimen los datos cuando se retira el consentimiento en que se basa el tratamiento	
Se suprimen los datos cuando se opone al tratamiento	
Se suprimen los datos cuando han sido tratados ilícitamente	
Se suprimen los datos cuando lo exige una obligación legal	
Se suprimen los datos cuando se obtienen en relación con la oferta de servicios de la sociedad de la información	

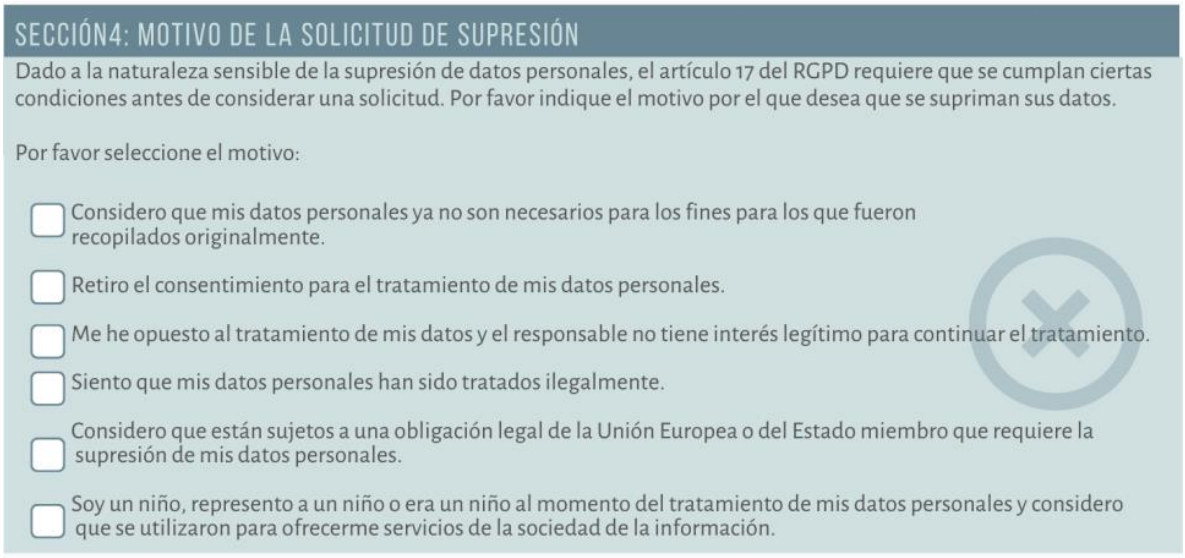
Por su parte, Dafne Méndez, a partir de evaluar una situación de derecho a la supresión conforme al artículo 17 del RGPD, propone un listado de verificación a ser considerados por organizaciones:[452]

[451] Agencia Española de Protección de Datos, *Listado de Cumplimiento Normativo*, [en línea] España, AEPD, s.a., [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://www.aepd.es/sites/default/files/2019-11/guia-listado-de-cumplimiento-del-rgpd.pdf* p. 8.

[452] Méndez Pérez, Stephany Dafne, *El Derecho al Olvido, análisis y propuesta de formulario*, [en línea] México, INFOTEC, 2021, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/486/1/TESIS%20DERECHO%20AL%20OLVIDO%20FINAL%20PARA%20IMPRESION%20-%20con%20autoizaci%C3%B3n%20de%20impresi%C3%B3n%281%29.pdf* pp. 141-142.

MEDIDAS PARA SOLICITUDES DE SUPRESIÓN	
Nuestra organización sabe cómo reconocer una solicitud de supresión o Derecho al Olvido	SI/NO
Nuestra organización entiende cuando es procedente aplicar el Derecho al Olvido	
Nuestra organización tiene política sobre cómo registrar las solicitudes que recibimos verbalmente	
Nuestra organización entiende cuándo se puede rechazar una solicitud y conoce la información que necesitamos proporcionar a las personas cuando lo hacemos.	
MEDIDAS PARA EL CUMPLIMIENTO DE SOLICITUDES DE SUPRESIÓN	
Nuestra organización cuenta con procesos para garantizar que respondamos a una solicitud de supresión sin demora indebida y dentro del mes siguiente a la recepción.	SI/NO
Nuestra organización conoce las circunstancias en que podemos extender el límite de tiempo para responder a una solicitud.	
Nuestra organización entiende que hay un énfasis particular en el derecho de supresión si la solicitud se refiere a datos recopilados de niños.	
Nuestra organización tiene procedimientos establecidos para informar a los destinatarios si borramos cualquier información que hayamos compartido con ellos.	
Nuestra organización tiene métodos apropiados para borrar la información	

Materializando este derecho en un formulario Dafne Méndez propone un formulario el cual en su parte sustantiva considera lo siguiente:[453]



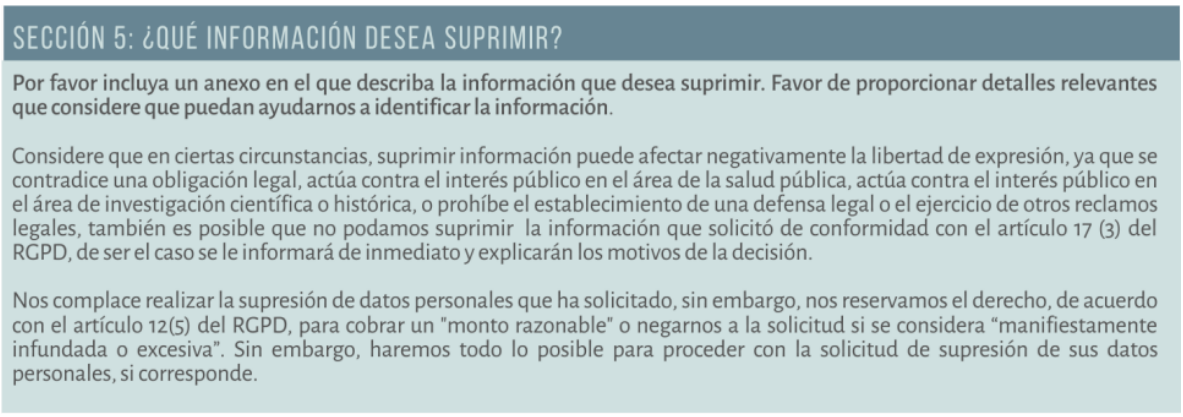
SECCIÓN4: MOTIVO DE LA SOLICITUD DE SUPRESIÓN

Dado a la naturaleza sensible de la supresión de datos personales, el artículo 17 del RGPD requiere que se cumplan ciertas condiciones antes de considerar una solicitud. Por favor indique el motivo por el que desea que se supriman sus datos.

Por favor seleccione el motivo:

- ☐ Considero que mis datos personales ya no son necesarios para los fines para los que fueron recopilados originalmente.
- ☐ Retiro el consentimiento para el tratamiento de mis datos personales.
- ☐ Me he opuesto al tratamiento de mis datos y el responsable no tiene interés legítimo para continuar el tratamiento.
- ☐ Siento que mis datos personales han sido tratados ilegalmente.
- ☐ Considero que están sujetos a una obligación legal de la Unión Europea o del Estado miembro que requiere la supresión de mis datos personales.
- ☐ Soy un niño, represento a un niño o era un niño al momento del tratamiento de mis datos personales y considero que se utilizaron para ofrecerme servicios de la sociedad de la información.

[453] *Ibídem*. p. 177.



SECCIÓN 5: ¿QUÉ INFORMACIÓN DESEA SUPRIMIR?

Por favor incluya un anexo en el que describa la información que desea suprimir. Favor de proporcionar detalles relevantes que considere que puedan ayudarnos a identificar la información.

Considere que en ciertas circunstancias, suprimir información puede afectar negativamente la libertad de expresión, ya que se contradice una obligación legal, actúa contra el interés público en el área de la salud pública, actúa contra el interés público en el área de investigación científica o histórica, o prohíbe el establecimiento de una defensa legal o el ejercicio de otros reclamos legales, también es posible que no podamos suprimir la información que solicitó de conformidad con el artículo 17 (3) del RGPD, de ser el caso se le informará de inmediato y explicarán los motivos de la decisión.

Nos complace realizar la supresión de datos personales que ha solicitado, sin embargo, nos reservamos el derecho, de acuerdo con el artículo 12(5) del RGPD, para cobrar un "monto razonable" o negarnos a la solicitud si se considera "manifiestamente infundada o excesiva". Sin embargo, haremos todo lo posible para proceder con la solicitud de supresión de sus datos personales, si corresponde.

Imagen: Formulario de motivos de solicitud de supresión de datos personales.
Tomado de: Méndez Pérez, Stephany Dafne, *El Derecho al Olvido, análisis y propuesta de formulario*, [en línea] México, INFOTEC, 2021, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/486/1/TESIS%20DERECHO%20AL%20OLVIDO%20FINAL%20PARA%20IMPRESION%20-%20con%20autoizaci%C3%B3n%20de%20impresi%C3%B3n%281%29.pdf* p. 177

Considero que apenas estamos garantizando el derecho de acceso y rectificación de datos personales; por ende, aún resta un largo trecho para ir garantizando los derechos de Cancelación y de Oposición; bastan más procedimientos y quejas que lleguen ante el INAI y por supuesto, falta que más juicios lleguen a los tribunales federales con el fin de que entren al estudio de fondo e ir creando una teoría nacional.

Por supuesto también falta más preparación de los abogados, como muestra pongo como ejemplo:

LICENCIADA
EN
DERECHO

M P
U V .

SERVICIO Y
ASESORAMIENTO
JURÍDICO

NO. 22_____34
Correo:
_____@gmail.com

Puebla, Pue. a 29 de Junio de 2021

S S A
PRESENTE

Saludos cordiales. Me dirijo hacia usted con el fin de solicitar, de la manera más atenta, la baja de un artículo de su blog de noticias En in " el cual se titula "Ho e e e ó o a ien os ci os u c u d n fue asegurado por la policía turística estatal de fecha, 14 de noviembre de 20

é f C a, mi representado, no siguió un proceso penal ya que no se encontraron pruebas suficientes para ello, motivo por el cual no se le siguieron lineas de investigación y no procedió a una audiencia inicial, lo contenido en el artículo mencionado carece de veracidad, esto en cuanto al supuesto hecho delictivo.

Dicho artículo, actualmente estigmatiza a mi cliente, es por ello que le solicito la indexación de la noticia puesto que se evitaría su divulgación indiscriminada, permanente y lesiva y así se dejaría de violar el artículo 16 parrafo II Constitucional que a la letra dice: "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" esto en relación con el artículo 22 de la "Ley Federal de protección de datos personales en posesión de los particulares", el cual plantea lo siguiente: "Cualquier titular, o en su caso, su representante legal, podrá ejercer los derechos de acceso, rectificación, cancelación y oposición previstos en la presente Ley. El ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio de otro. Los datos personales deben ser resguardados de tal manera que permitan el ejercicio sin dilación de estos derechos."

Es por todo lo anterior que reitero mi solicitud para que sea eliminado el artícu o de u blog de noticias "En n e o e el cual se titu a H m e qu e zó oc ento asci o a na u d na, ue a e u do o la p l c a urís ca s de fecha, 14 de mbre de 2 por ser contrario también a otros derechos como lo son la intimidad, la privacidad, el honor y la propia imagen, derechos que han sido vulnerados en conjunto o colateralmente y no de manera aislada

Sin más por el momento, agradezco de antemano su atención.

ABOGADA M P___ U___ V

De este texto, podemos advertir algunas imprecisiones, como el manejo de la palabra indexación, en lugar de desindexación; la falta de pedir la cancelación y posterior supresión de datos, pedir la oposición al mismo tiempo, ya que se pueden ejercer varios de los derechos ARCO de manera simultáneo; no hace referencia al aviso de privacidad del responsable, entre otros. Cabe señalar que este texto lo encontré casualmente en una red de Telegram de manera libre lo que puede conllevar a otro tipo de violaciones por parte de la profesional del Derecho.

Por lo anterior, considero que apenas estamos garantizando el derecho de acceso y rectificación de datos personales, por ende, aún resta un largo trecho para ir garantizando los derechos de cancelación y de oposición; hace mucha falta capacitación especializada a licenciados en Derecho, más procedimientos y quejas que lleguen ante el INAI y por supuesto, falta que más juicios lleguen a los tribunales federales con el fin de que entren al estudio de fondo e ir creando una teoría nacional.

5.3.3.2. Seguridad y Ciberseguridad.

Contrario a lo que pudiésemos imaginar, en materia de seguridad de datos personales, México ha tenido avances significativos en esta materia. No obstante, el uso inapropiado por parte de los responsables del tratamiento de datos personales, así como el desconocimiento de las Leyes de protección de Datos Personales, ocasionan un bajo nivel de confianza en los titulares, tal como lo demuestra la ENAID 2019.

Como se puede apreciar, existe poco conocimiento de la LFPDPPP por un lado, y por otro, se aprecia no solamente prácticas inadecuadas por parte de responsables de datos, sino que cada vez los derechos de oposición y cancelación van en aumento de forma significativa; lo cual no solo pone de manifiesto la parte del derecho al olvido; sino que también obliga a los responsables del tratamiento de datos en contar con mayor seguridad en el manejo de bases de datos, que es la fuente de donde se realizan llamadas, ya sea para prospectar o bien para ofrecer servicios.

En este tenor, y siguiendo la premisa de que en México contamos con otras normas y leyes que obligan directa o indirectamente al cuidado y seguridad de datos personales en el ámbito privado o de particulares, tales como:

1) NOM-024-SSA3-2012, Sistemas de información de registro electrónico para la salud. Intercambio de información en salud (DOF: 30/nov/2012)
2) NOM-151-SCFI-2016, Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos (cancela la NOM-151-SCFI-2002). (DOF: 30/03/2017)
3) NMX-I-27018-NYCE-2016, Tecnologías de la información-Técnicas de seguridad-Código de práctica para la protección de datos personales (DP) para proveedores de servicios de nubes públicas (DOF: 26/08/2016)

4) Ley para Regular las Sociedades de Información Crediticia
5) Ley Federal de Protección al Consumidor
6) Ley de los Derechos de las Personas Adultas Mayores
7) Ley Federal para Prevenir y Eliminar la Discriminación
8) Ley de Concursos Mercantiles
9) Ley General de Turismo
10) Ley de Protección y Defensa al Usuario de Servicios Financieros
11) Ley general para la inclusión de las personas con discapacidad
12) Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita
13) Ley de Ahorro y Crédito Popular
14) Ley General de los Derechos de Niñas, Niños y Adolescentes
15) Ley General de Salud
16) Ley Aduanera
17) Ley de Comercio Exterior
18) Ley de Aviación Civil
19) Ley General de Cultura Física y Deporte
20) Ley Federal de Telecomunicaciones y Radiodifusión
21) Ley de Hidrocarburos
22) Ley para Regular las Instituciones de Tecnología Financiera
23) Ley de Instituciones de Seguros y de Fianzas
24) Ley sobre el Contrato de Seguro
25) Ley del Mercado de Valores
26) Ley General de Organizaciones y Actividades Auxiliares del Crédito
27) Ley de Uniones de Crédito
28) Ley Federal de Armas de Fuego y Explosivos
29) Ley de Vías Generales de Comunicación
30) Ley Agraria
31) Leyes de Propiedad en Condominio Estatales
32) Leyes de Seguridad Privada ya sea Federal o Estatales
33) Leyes de Videovigilancia Estatales
34) Leyes de Voluntariado o Voluntariado Social Estatales
35) Leyes de Albergues Privados Estatales
36) Leyes de Protección Animal Estatales
37) Leyes de Cuidados Alternativos para Niños o sus equivalentes Estatales
38) Ley para la Prevención, Tratamiento y Control de la Diabetes o sus equivalentes Estatales
39) Leyes de Seguridad Alimentaria y Nutricional o sus equivalentes Estatales
40) Reglamento de la Ley General de Desarrollo Forestal Sustentable.

Evidentemente, la normatividad descrita arriba, se aplica según el giro o actividad del responsable; es decir además de los dispuesto por la LFPDPPP, su reglamento, etc.; se debe adicionar la normatividad *ex profeso* que le corresponda, con lo cual se deberá gestionar el sistema de seguridad correspondiente.

Ahora bien, además de la legislación y normas descritas arriba, así como de la LFPDPPP, su reglamento, los lineamientos del aviso de privacidad y los parámetros de autorregulación vinculante; el INAI ha desarrollado una serie de formatos, recomendaciones, guías, estudios, manuales, entre otros, que también forman parte del sistema de seguridad para datos personales como:

1. Recomendaciones en materia de seguridad de datos personales. (DOF: 30/10/2013)
2. Documentos de Facilitación
    a. Guía para Instrumentar Medidas Compensatorias (Mayo 2016)
    b. Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Junio 2016)
    c. Guía para orientar el debido tratamiento de datos personales en la actividad de cobranza extrajudicial (Agosto 2016)
3. Sistema de Gestión de Seguridad de Datos Personales
    a. Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales (Junio 2015)
    b. Guía para el Borrado Seguro de Datos Personales (Junio 2016)
    c. Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas (Junio 2015)
    d. Manual en materia de seguridad basada en un entorno Microsoft® para MiPyMEs y organizaciones pequeñas mexicanas (Noviembre 2015)
4. Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales (Octubre 2018)
5. Conformidad de contratos de adhesión de servicios de cómputo en la nube vs los criterios mínimos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales (Febrero 2021)
6. Recomendaciones para el tratamiento de datos personales y cumplir con el deber de seguridad para Instituciones de Tecnología Financiera (ITF) (Febrero 2021)
7. Recomendaciones para reconocer las principales amenazas a los datos personales a partir de la valoración respecto al riesgo (Abril 2021)
8. Guía de esquemas de autorregulación en materia de protección de datos personales (Diciembre 2016)
9. Guía para la elaboración de evaluaciones de impacto a la privacidad (Diciembre 2020)
10. Guía para el tratamiento de datos biométricos (Marzo 2018)
11. Código de las buenas prácticas para orientar el tratamiento en línea de Datos Personales de niñas, niños y adolescentes (Octubre 2020)
12. Recomendaciones para el manejo de incidentes de seguridad de datos personales (Junio 2018)
13. Tabla de equivalencia funcional entre estándares de seguridad y la LFPDPPP, su Reglamento y las Recomendaciones en materia de seguridad de datos personales – Completa (Junio 2015)

14. Metodología de Análisis de Riesgo BAA (Junio 2015)
15. Toolkit de Concientización de Seguridad de Datos Personales para Responsables del Sector Privado (Agosto 2021)

De estas herramientas es de destacar el "*Toolkit*" de Concientización, el cual es el más reciente y consiste en "ayudar a los responsables y encargados del tratamiento de datos personales del sector privado a cumplir con el **deber de seguridad** establecido en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), concretamente el referido a la obligación de establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado."[454]

Este *Toolkit*, tiene el siguiente esquema:[455]

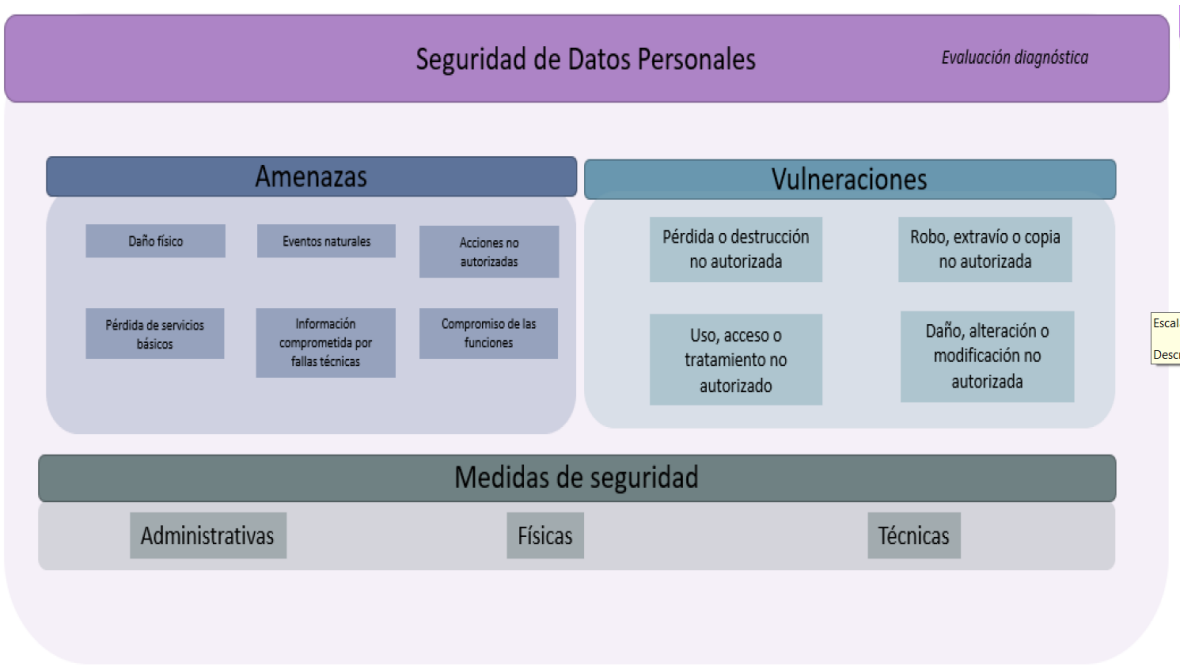


Imagen: Módulos que integran el *Toolkit* en materia de seguridad para el cumplimiento de la LFPDPPP.
Tomado de: INAI, *Manual de Implementación*, en "Toolkit de Concientización de Seguridad de Datos Personales para Responsables del Sector Privado", México, INAI, 2021, [fecha de consulta: 5 de diciembre de 2022] Disponible en: en https://home.inai.org.mx/?page_id=3418 p.5.

Además, a lo largo de los módulos, se manejan términos como los de ciberseguridad; terrorista informático, *Hacker, Hacktivista, Cracker*, criminales computacionales, exfiltración de datos, entre otros.

---

[454] INAI, *Manual de Implementación, en "*Toolkit de Concientización de Seguridad de Datos Personales para Responsables del Sector Privado", México, INAI, 2021, Descarga en formato .zip, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://home.inai.org.mx/?page_id=3418* p.3.
[455] *Ibídem* p. 5.

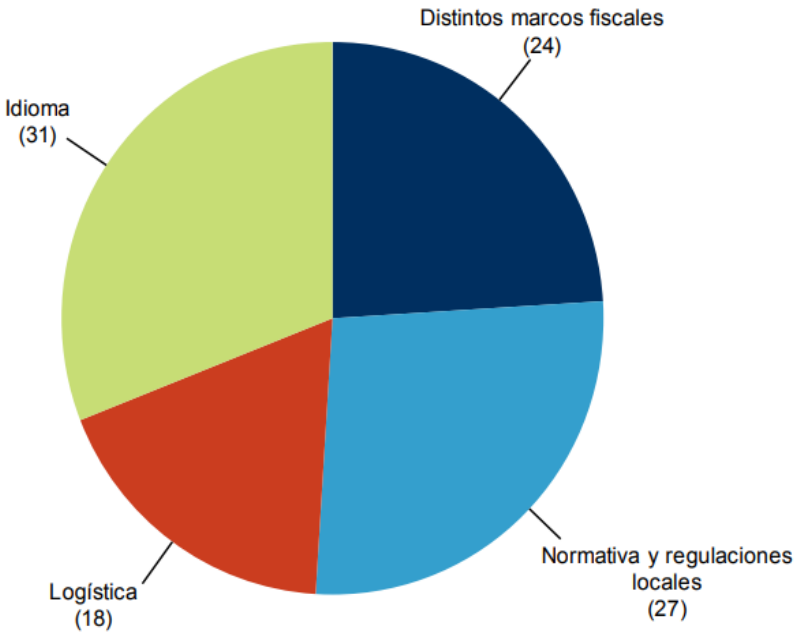
No existe día en que no se reporten fallas de plataformas por ataques cibernéticos o ataques informáticos, robo de información, terrorismo informático, suplantación de identidad y un sinfín de malas prácticas y ciberdelitos.

La Comisión Económica para América Latina y el Caribe (CEPAL) indica que “para avanzar en el desarrollo de la economía digital, es necesario contar con un mercado digital integrado”[456]; ya que si bien el uso del internet ha facilitado el comercio existen una serie de factores que afectan su expansión como marcos fiscales, idioma, logística y por supuesto el marco regulador, el cual abarca aspectos como las leyes de derechos al consumidor, así como la protección de datos personales.

La CEPAL grafica como principales barreras al comercio electrónico transfronterizo lo siguiente:[457]

Principales barreras al comercio electrónico transfronterizo a nivel mundial

(En porcentajes de encuestados)



Fuente: K. McDermott y Payvision, *Key Business Drivers and Opportunities in Cross-Border Ecommerce*, 2015 [en línea] http://hollandfintech.com/wp-content/uploads/2015/11/key-business-drivers-and-opportunities-2015.pdf.

[456] Comisión Económica para América Latina y el Caribe, *Ciencia, tecnología e innovación en la economía digital. La situación de América Latina y el Caribe*, [en línea], Chile, CEPAL, 2016, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://repositorio.cepal.org/bitstream/handle/11362/40530/3/S1600833_es.pdf* p.68.
[457] *Ídem.*

Por lo antes expuesto, actualmente se tiene que hablar de la ciberseguridad; la cual "se refiere al uso seguro y responsable de los productos de la tecnología de la información y la comunicación (TIC), incluyendo Internet, los dispositivos móviles y de comunicación y los instrumentos tecnológicos diseñados para guardar, compartir o recibir información, por ejemplo, los teléfonos móviles, las cámaras digitales, etc."[458]

Ahora bien, en el mensaje del Gerente de Instituciones para el Desarrollo del BID, Moisés J. Schwartz en su informe del reporte de Ciberseguridad de 2020 del Banco Interamericano de Desarrollo, mencionó que "la crisis propiciada a principios de 2020 por la pandemia del COVID-19 ha puesto de relieve nuestra dependencia de una infraestructura vital que, para la gran mayoría de los ciudadanos, resulta invisible o su existencia pasa prácticamente desapercibida. […] Las políticas de ciberseguridad son fundamentales para salvaguardar los derechos de los ciudadanos en el ámbito digital, tales como la privacidad, la propiedad, así como para aumentar la confianza de los ciudadanos en las tecnologías digitales, y que estos puedan sentirse cómodos accediendo a dichas tecnologías."[459]

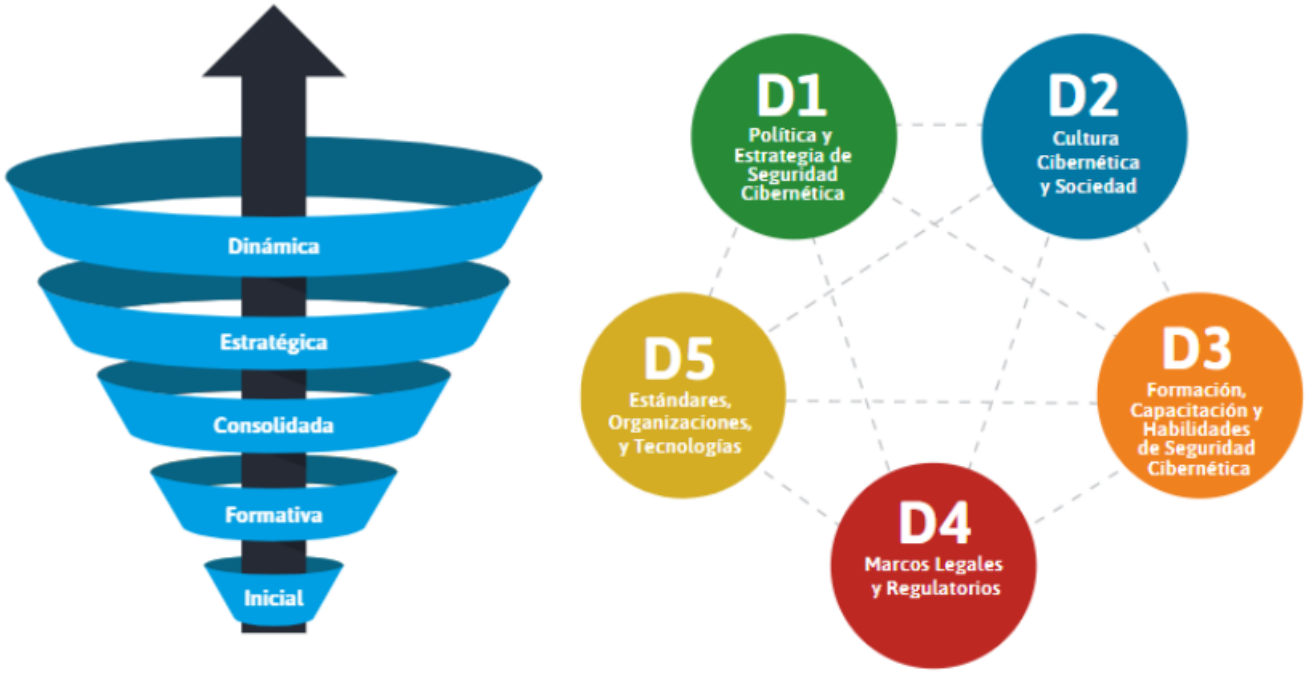


Imagen: Modelo de madurez de la capacidad de ciberseguridad I.
Tomado de: Banco Interamericano de Desarrollo, *Ciberseguridad, riesgos, avances y el camino a seguir en América Latina y el Caribe*, [en línea] BID, 2020, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf* pp. 42 y 44.

[458] Giant, Nikki, *Ciberseguridad para la i-generación. Usos y riesgos de las Redes Sociales y sus aplicaciones*, España, Narcea, 2007, p. 8.
[459] Banco Interamericano de Desarrollo, *Ciberseguridad, riesgos, avances y el camino a seguir en América Latina y el Caribe*, [en línea] BID, 2020, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf* p. 11.

En el Informe de Ciberseguridad del BID, se presenta un modelo de madurez de la capacidad de ciberseguridad, el cual busca ofrecer una evaluación del nivel de madurez de las capacidades de ciberseguridad de un país; el cual está basado en cinco etapas que van desde la más básica (inicial), hasta la más avanzada (dinámica), tal como se aprecia en los siguientes cuadros:[460]

Dimensión 1 Política y Estrategia de Ciberseguridad (Diseño de estrategia y resiliencia de ciberseguridad)	**D1.1** Estrategia Nacional de Ciberseguridad **D1.2** Respuesta a Incidentes **D1.3** Protección de Infraestructura Crítica (IC) **D1.4** Gestión de Crisis **D1.5** Defensa Cibernética **D1.6** Redundancia de Comunicaciones
Dimensión 2 Cultura Cibernética y Sociedad (Fomentar una cultura de ciberseguridad responsable en la sociedad)	**D2.1** Mentalidad de Ciberseguridad **D2.2** Confianza y Seguridad en Internet **D2.3** Comprensión del Usuario de la Protección de Información Personal en Línea **D2.4** Mecanismos de Presentación de Informes **D2.5** Medios y Redes Sociales
Dimensión 3 Educación, Capacitación y Habilidades en Ciberseguridad (Desarrollo del conocimiento de ciberseguridad)	**D3.1** Sensibilización **D3.2** Marco para la Educación **D3.3** Marco para la Formación Profesional

[460] *Ibidem.* pp. 42 a 44.

Dimensión 4 Marcos Legales y Regulatorios (Creación de marcos legales y regulatorios efectivos)	**D4.1** Marcos Legales **D4.2** Sistema de Justicia Penal **D4.3** Marcos de Cooperación Formal e Informal para Combatir el Delito Cibernético
Dimensión 5 Estándares, Organizaciones y Tecnologías (Control de riesgos a través de estándares, organizaciones y tecnologías)	**D5.1** Adhesión a los Estándares **D5.2** Resiliencia de Infraestructura de Internet **D5.3** Calidad del Software **D5.4** Controles Técnicos de Seguridad **D5.5** Controles Criptográficos **D5.6** Mercado de Ciberseguridad **D5.7** Divulgación Responsable

Imagen: Modelo de madurez de la capacidad de ciberseguridad II.
Tomado de: Banco Interamericano de Desarrollo, *Ciberseguridad, riesgos, avances y el camino a seguir en América Latina y el Caribe*, [en línea] BID, 2020, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf* pp. 43 y 44.

En este informe colocan a México de la siguiente forma:[461]

[461] *Ibidem*, p. 124-127.

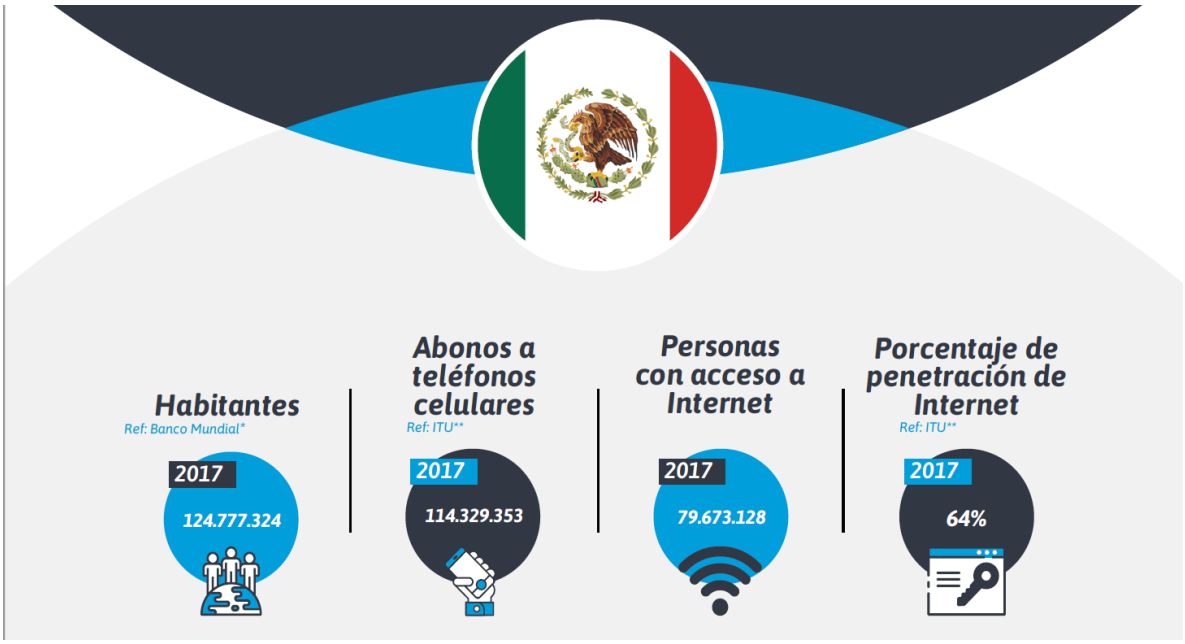


Imagen: Indicadores en ciberseguridad en México I.

Tomado de: Banco Interamericano de Desarrollo, *Ciberseguridad, riesgos, avances y el camino a seguir en América Latina y el Caribe*, [en línea] BID, 2020, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf* p. 124.

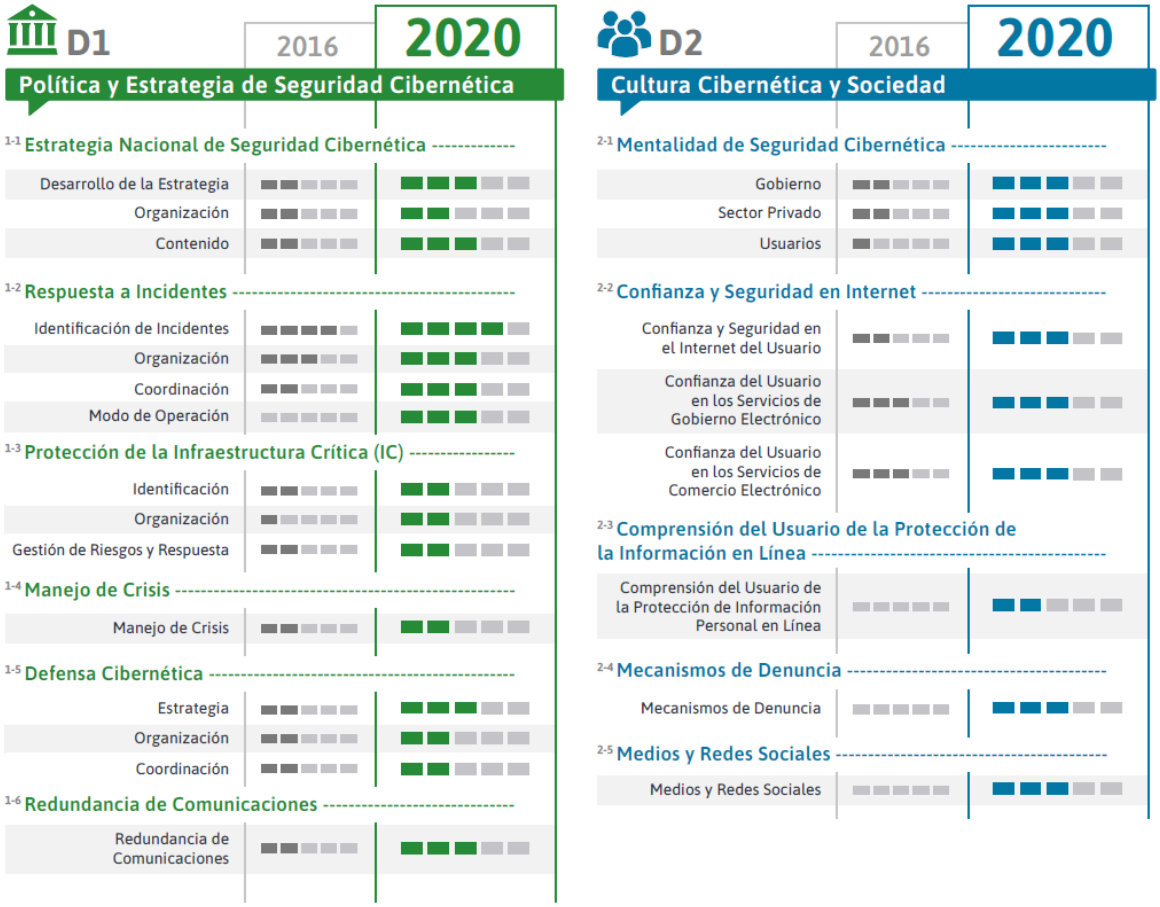


Imagen: Indicadores en ciberseguridad en México II.
Tomado de: Banco Interamericano de Desarrollo, *Ciberseguridad, riesgos, avances y el camino a seguir en América Latina y el Caribe*, [en línea] BID, 2020, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf* pp. 126-127

.

Ahora bien, la preocupación por la ciberdelincuencia si bien se puede decir que es relativamente reciente, tiene como primera fuente de Derecho Internacional, el Convenio sobre la Ciberdelincuencia, conocido como Convenio de Budapest, fue firmado en Budapest, Hungría el 23 de noviembre de 2001, y entró en vigor el 01 de

julio de 2004.

Se destaca el capítulo II, sección 1, cuyo contenido es el siguiente:[462]

> **Capítulo II - Medidas que deberán adoptarse a nivel nacional**
> Sección 1 - Derecho penal sustantivo
> - Título 1 – Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos (acceso ilícito, interceptación ilícita, ataques a la integridad de los datos, ataques a la integración del sistema, abuso de los dispositivos)
> - Título 2 – Delitos informáticos (falsificación informática, fraude informático)
> - Título 3 – Delitos relacionados con el contenido (pornografía infantil)
> - Título 4 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines
> - Título 5 – Otras formas de responsabilidad y de sanción (tentativa y complicidad, responsabilidad de las personas jurídicas, sanciones y medidas)

El informe explicativo de este convenio manifiesta que dicho convenio tiene como finalidad primordial: 1) armonizar los elementos de los delitos conforme al derecho sustantivo penal de cada país y las disposiciones conexas en materia de delitos informáticos; 2) establecer conforme al derecho procesal penal de cada país los poderes necesarios para la investigación y el procesamiento de dichos delitos, así como también de otros delitos cometidos mediante el uso de un sistema informático o las pruebas conexas que se encuentren en formato electrónico, 3) establecer un régimen rápido y eficaz de cooperación internacional.[463]

La sección 1 del capítulo II (Derecho penal sustantivo) abarca las disposiciones relativas a los delitos y otras disposiciones conexas referentes al ámbito de los delitos informáticos o los delitos relacionados con el empleo de ordenadores. En primer lugar, define nueve delitos agrupados en cuatro categorías diferentes y más tarde versa sobre las responsabilidades y sanciones conexas. El Convenio define los siguientes delitos: acceso ilícito, interceptación ilícita, ataques a la integridad de los datos, ataques a la integridad del sistema, abuso de los dispositivos, falsificación informática, fraude informático, delitos relacionados con la pornografía infantil y delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.[464]

Posteriormente, surgió el Protocolo Adicional al Convenio sobre Ciberdelincuencia,

---

[462] Consejo de Europa, *Convenio sobre la Ciberdelincuencia*, [en línea] CE, Serie de Tratados Europeos No. 185, Budapest, 23-11-2001, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://www.oas.org/juridico/english/cyb_pry_convenio.pdf*

[463] Consejo de Europa, *Informe Explicativo del Convenio sobre la Ciberdelincuencia*, [en línea] CE, s.d., s.a., [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://rm.coe.int/16802fa403* p. 1.

[464] *Ídem*.

cuya finalidad es completar, las disposiciones del Convenio sobre la Ciberdelincuencia, abierto a la firma en Budapest el 23 de noviembre de 2001 (en lo sucesivo denominado «el Convenio»), por lo que respecta a la tipificación penal de los actos de índole racista y xenófoba cometidos mediante sistemas informáticos.[465]

Actualmente, en 2021, el mismo Consejo de Europa tiene en preparación el Segundo Protocolo adicional al Convenio de Budapest sobre la Delincuencia, relativo a la cooperación reforzada y la divulgación de pruebas electrónicas. Este proyecto, relativo al segundo protocolo plantea en su capítulo III un artículo relativo a la Protección de datos personales en los siguientes numerales:[466]

1. Calidad e integridad.
2. Datos sensibles.
3. Periodos de conservación.
4. Decisiones automatizadas.
5. Seguridad de los datos e incidentes de seguridad.
6. Mantenimiento de registros.
7. Intercambio de información dentro de una Parte.
8. Transferencia ulterior a otro Estado u organización internacional.
9. Transparencia y notificación.
10. Acceso y rectificación.

Es importante destacar que la Convención sobre Ciberseguridad permite la adición de otros países además de los europeos, como en el caso del Convenio 108 de Europa; pero además se tienen países observadores. Para lo anterior sirven los

[465] Consejo de Europa, *Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos, hecho en Estrasburgo el 28 de enero de 2003*, [en línea] España, Boletín Oficial del Estado, 2015, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://www.boe.es/boe/dias/2015/01/30/pdfs/BOE-A-2015-793.pdf*

[466] Consejo de Europa, *Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo al refuerzo de la cooperación y de la divulgación de pruebas electrónicas, Proyecto de Protocolo, versión 2*, T-CY (2020)7 [en línea] C.E., 2021, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://rm.coe.int/0900001680a27dbe*

siguientes cuadros:[467]

Imagen: Países observadores de la Convención de Budapest.
Tomado de: Consejo de Europa, *Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY*, [en línea] C.E., s.a., [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://www.coe.int/en/web/cybercrime/parties-observers*

Imagen: Países parte de la Convención de Budapest.
Tomado de: Consejo de Europa, *Parties/Observers to the Budapest Convention and Observer Organizations to the T-CY*, [en línea] C.E., s.a., [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://www.coe.int/en/web/cybercrime/parties-observers*

Ahora bien, México no ha suscrito dicho convenio, a pesar de que en diferentes ocasiones se ha exhortado al Ejecutivo a adherirse al mismo. La última corresponde a la sala de Comisiones de la Cámara de Senadores a los 25 días del mes de febrero de 2021 en los siguientes términos:

> ACUERDO
> ÚNICO. El Senado de la República exhorta respetuosamente a las autoridades del Poder ejecutivo Federal a fin de que se concluya la etapa de evaluación del marco jurídico vigente que permitiría iniciar los trabajos necesarios para la adhesión de México al Convenio

[467] Consejo de Europa, *Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY*, [en línea] C.E., s.a., [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://www.coe.int/en/web/cybercrime/parties-observers*

sobre la Ciberdelincuencia, o Convenio de Budapest.[468]

Danya Centeno establece posibles incompatibilidades que versan en las siguientes áreas:[469]

1) Implementación de la parte sustantiva del Convenio de Budapest.
2) Principio de exacta aplicación de la Ley Penal en México.
3) Principio de Culpabilidad
4) Implementación de los delitos previstos en el Convenio de Budapest.

Otros esfuerzos internacionales que tienen que ver con estudiar la armonización de legislación sobre ciberseguridad está la UNCTAD, la cual, en su último estudio de 2015, muestra el estado de la ciber legislación de los países de América Latina de la siguiente forma:[470]

País	Transaccio-neselectróni-cas/ firmas electrónicas	Protección al Consumidor	Protección de Datos	Propiedad Intelec-tual	Nombres de dominio	Delitos Informáticos y Seguridad de la Información
Argentina						
Bolivia						
Brasil						
Chile						
Colombia						
Costa Rica						
Cuba						
Ecuador						
El Salvador						
Guatemala						
Haití						
Honduras						
México						
Nicaragua						
Panamá						
Paraguay						
Perú						
República Dominicana						
Uruguay						
Venezuela						

Fuente: UNCTAD, 2015.

[468] Cámara de Senadores, *Dictamen de la Comisión de Relaciones Exteriores, a los puntos de acuerdo por los que se exhorta al Ejecutivo Federal a iniciar los trabajos necesarios para la adhesión de México al Convenio sobre la Ciberdelincuencia, o Convenio de Budapest*, [en línea] México, Senado, 2021, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://infosen.senado.gob.mx/sgsp/gaceta/64/3/2021-03-11-1/assets/documentos/Dict_Com_Relaciones_Exteriores_Ciberdelincuencia_Convenio_Budapest.pdf* p. 18.

[469] Centeno, Danya, *México y el Convenio de Budapest: Posibles Incompatibilidades*, [en línea], México, Derechos Digitales, 2018, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://www.derechosdigitales.org/wp-content/uploads/minuta_r3d.pdf*

[470] Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, *Examen de la armonización de la ciberlegislación en América Latina*, [en línea], UNCTAD, 2015, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://unctad.org/es/system/files/official-document/dtlstict2015d4_es.pdf* pp. 2-3.

Valores Normativos:

Valor	Enunciado	Descripción
	Facilita el comercio electrónico	La legislación es acorde con las mejores prácticas internacionales acordadas por organismos internacionales, tales como la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), la Organización Mundial de la Propiedad Intelectual (OMPI), la Organización Mundial del Comercio (OMC), la Unión Internacional de Telecomunicaciones (UIT), la Red Iberoamericana de Protección de Datos Personales, el Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OEA) / Comité Interamericano contra el Terrorismo (CICTE), el Consejo de Europa y la Organización para la Cooperación y el Desarrollo Económicos (OCDE).
	Facilita parcialmente el comercio electrónico.	Existe legislación en la materia, sin embargo, no es acorde con las mejores prácticas internacionales. Hace falta homologación normativa.
	No existe legislación.	

Imagen: Estado de la ciberlegislación de los países de América Latina.
Tomado de: Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, *Examen de la armonización de la ciberlegislación en América Latina*, [en línea], UNCTAD, 2015, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://unctad.org/es/system/files/official-document/dtlstict2015d4_es.pdf* pp. 2-3.

Actualmente, México asumió una Vicepresidencia para la zona de México y Centroamérica en la Séptima Conferencia Ministerial sobre la Sociedad de la Información de América Latina y el Caribe, realizada del 23 al 26 de noviembre de 2020.[471]

Los trabajos de esta conferencia se centraron en la redacción conjunta de la Agenda Digital para América Latina y el Caribe (eLAC 2022) que traza una ruta de acción en materia tecnológica para los siguientes dos años. La Agenda eLAC 2022, se conforma de un total de 39 objetivos organizados en nueve áreas de acción que se enlistan a continuación:[472]

1) Infraestructura digital.
2) Transformación digital y economía digital.
3) Gobierno digital.
4) Inclusión, competencias y habilidades digitales.
5) Tecnologías emergentes para el desarrollo sostenible.
6) Confianza y seguridad digital.
7) Mercado digital regional.
8) Cooperación regional digital.
9) Enfrentar la pandemia y facilitar la recuperación y reactivación económica.

No obstante a lo anterior, es importante mencionar que México tiene un programa de ciberseguridad de 2017, mismo que no se ha actualizado. El objetivo general de la Estrategia Nacional de Ciberseguridad (ENCS) es identificar y establecer las acciones en materia de ciberseguridad aplicables a los ámbitos social, económico y

[471] Gobierno de México, *VII Conferencia Ministerial sobre la Sociedad de la Información de América Latina y el Caribe*,[en línea], México, Coordinación de Estrategia Digital Nacional, 2021, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://www.gob.mx/cedn/articulos/vii-conferencia-ministerial-sobre-la-sociedad-de-la-informacion-de-america-latina-y-el-caribe*
[472] *Ídem*.

político que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las TIC de manera responsable para el desarrollo sostenible del Estado Mexicano.[473]

Para cumplir con el objetivo general, se establecen 5 objetivos estratégicos:

1. Sociedad y derechos.
2. Economía e innovación.
3. Instituciones públicas.
4. Seguridad pública.
5. Seguridad nacional.

Para el desarrollo de la ENCS se consideran tres principios rectores:

A. Perspectiva de derechos humanos.
B. Enfoque basado en gestión de riesgos.
C. Colaboración multidisciplinaria y de múltiples actores.

Para alcanzar los objetivos estratégicos se desarrollarán 8 ejes transversales:

1. Cultura de ciberseguridad.
2. Desarrollo de capacidades.
3. Coordinación y colaboración.
4. Investigación, desarrollo e innovación TIC.
5. Estándares y criterios técnicos.
6. Infraestructuras críticas.
7. Marco jurídico y autorregulación.
8. Medición y seguimiento.

En una etapa inicial, la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE) a través de la Subcomisión de Ciberseguridad sería la encargada de coordinar al Gobierno de la República y articular los esfuerzos de los diferentes actores para la implementación y seguimiento de la Estrategia.
La Estrategia Nacional de Ciberseguridad es de naturaleza transversal y se articuló con otros programas y estrategias y se desprende de lo señalado en el propio Plan Nacional de Desarrollo 2013-2018, en apego a los valores y principios que establece la Constitución Política de los Estados Unidos Mexicanos.[474]

[473] Gobierno Federal, *Estrategia Nacional de Ciberseguridad*, [en línea] México, 2017, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://intranet.inaes.gob.mx/pdf/CiberSeguridad/Estrategia_Nacional_Ciberseguridad.pdf* p. 4.
[474] *Ibidem*. p. 15.

Imagen: Naturaleza transversal de la Estrategia Nacional de Ciberseguridad.
Tomado de: Gobierno Federal, *Estrategia Nacional de Ciberseguridad*, [en línea] México, 2017, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://intranet.inaes.gob.mx/pdf/CiberSeguridad/Estrategia_Nacional_Ciberseguridad.pdf* p. 15.

Aunque desafortunadamente, esta estrategia ha quedado más en el papel, se pueden destacar dos acciones principales en materia de ciberseguridad por parte de las autoridades federales.

En primer lugar, destaca el Instituto Federal de Telecomunicaciones del cual se mencionan tres disposiciones normativas relativas a la ciberseguridad:

1) Plan de Acciones en materia de Ciberseguridad (noviembre 2018)[475]
2) Estrategia IFT 2020-2024 (31 de julio de 2020)[476]
3) Estrategia IFT 2021-2025 (diciembre de 2020)[477]

Se destacan que estas estrategias de ciberseguridad incluyen protección de datos personales.

La segunda acción es la actuación de la policía cibernética creada durante el gobierno del entonces presidente Vicente Fox, ha venido fortaleciendo su presencia, alcances y colaboración con las entidades federativas.

---

[475] Instituto Federal de Telecomunicaciones, *Plan de acciones en materia de* ciberseguridad, [en línea], México, IFT, 2018, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://ciberseguridad.ift.org.mx/files/guias_y_estudios/5_upr_planaccionesciberseguridad.pdf*

[476] Instituto Federal de Telecomunicaciones, *Estrategia IFT 2020-2024*, [en línea], México, IFT, 2020, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *http://www.ift.org.mx/sites/default/files/industria/temasrelevantes/16510/documentos/hrparaconsultapublicadefinitivascv390820_0.pdf*

[477] Instituto Federal de Telecomunicaciones, *Estrategia IFT 2021-2025*, [en línea], México, IFT, 2020, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *http://www.ift.org.mx/sites/default/files/contenidogeneral/transparencia/estrategia20202025.pdf*

Tan solo en el anterior Plan Nacional de Desarrollo 2013-2018 se asentaron modelos y estrategias de ciberseguridad como se aprecia a continuación:

Imagen: Policía cibernética y estrategia de ciberseguridad en el programa nacional de seguridad pública.
Tomado de: Gobierno Federal, *Modelo homologado de unidades de policía cibernética*, [en línea] México, 2017., [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://www.gob.mx/cms/uploads/attachment/file/189189/Modelo_homologado_unidades_policia_cibernetica.pdf* p. 2.

De hecho, las Unidades de Policía Cibernética se han reunido desde 2015, durante las actividades de la Semana Nacional de Ciberseguridad que año con año organiza la División Científica en transición a la Guardia Nacional. En 2015, los Secretarios de Seguridad Pública firmaron un acuerdo de colaboración con la Policía Cibernética para fortalecer las capacidades de Ciberseguridad en la lucha contra el Cibercrimen.[478]

De hecho en 2017 se publicó el documento denominado Modelo Homologado de Unidades de Policía Cibernética, el cual tuvo como objetivo "sentar las bases de coordinación para incrementar la capacidad del Estado Mexicano en la prevención y atención de delitos cibernéticos, proponiendo un modelo de operación para las Policías Cibernéticas Estatales, así como los canales de comunicación que sirvan como marco de implementación para la creación y fortalecimiento de las Policías Cibernéticas del país mediante la capacitación y especialización de policías en activos."[479]

[478] Secretaría de Seguridad Ciudadana, *Avances de la Implementación del Modelo Homologado de Unidades de Policía Cibernética*, [en línea] México, SSCPC-Guardia Nacional, 2020, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://www.gob.mx/cms/uploads/attachment/file/527384/13_GUARDIA_NAL_POL_CIBERNe_TICA_CAPACITACI_N_2020.pdf* p. 2.
[479] Gobierno Federal, *Modelo homologado de unidades de policía cibernética*, [en línea] México,

Ahora bien, en cuanto a la legislación sobre la materia, apenas tenemos disposiciones aisladas como las siguientes:

En el Código Penal Federal el 17 de mayo de 1999 se publicó en el DOF, las modificaciones y añadieron artículos al título noveno de la siguiente forma:

> TITULO NOVENO
> Revelación de secretos y acceso ilícito a sistemas y equipos de informática
> CAPITULO I
> Revelación de secretos
> CAPITULO II
> Acceso ilícito a sistemas y equipos de informática
>
> Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.
> Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.
>
> Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.
>
> Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.
>
> Artículo 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.
>
> Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.
>
> Artículo 211 bis 4.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún

2017., [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://www.gob.mx/cms/uploads/attachment/file/189189/Modelo_homologado_unidades_policia_cibernetica.pdf* p. 8.

mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Artículo 211 bis 6.- Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.

Artículo 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

No obstante, desde la adición de delitos específicamente informáticos en el ordenamiento penal mexicano, se han llevado a cabo diversas iniciativas de ley y decreto, las cuales, de manera no limitativa, se enlistan a continuación:[480]

- 12 abril 2005: Iniciativa que reforma, adiciona y deroga diversas disposiciones del código penal federal, del código federal de procedimientos penales, de la ley federal contra la delincuencia organizada y de la ley de la policía federal preventiva, en materia de delitos cibernéticos y de delitos contra menores.
- 13 abril 2010: De la Sen. Claudia Sofía Corichi García, del grupo parlamentario del partido de la revolución democrática, la que contiene proyecto de decreto por el que se adiciona un párrafo a la fracción XVI del artículo 64 de la ley federal de telecomunicaciones y se agrega un capítulo III al título noveno del código penal federal.

[480] Llamas Covarrubias, Jersain, *Observaciones y Estudio de la iniciativa que expide la Ley General de Ciberseguridad en México*, [en línea] México, Revista Foro Jurídico, secc. Noticias, septiembre 07, 2020, [fecha de consulta: 5 de diciembre de 2022] Disponible en: *https://forojuridico.mx/observaciones-y-estudio-de-la-iniciativa-que-expide-la-ley-general-de-ciberseguridad-en-mexico/*

- 15 febrero 2012: De la comisión de justicia con proyecto de decreto que reforma y adiciona diversas disposiciones al código penal federal.
- 28 marzo 2012: Proyecto de decreto por el que se reforman y adicionan diversas disposiciones al código penal federal en materia de delitos en contra de medios o sistemas informáticos.
- 18 abril 2012: Proyecto de dictamen de las comisiones unidas de justicia y de estudios legislativos, segunda, el que contiene proyecto de decreto por el que se reforman y adicionan diversas disposiciones al código penal federal.
- 16 abril 2013: Reforma y adiciona diversas disposiciones de los códigos penal federal, y federal de procedimientos penales, así como de las leyes general para prevenir, sancionar y erradicar los delitos en materia de trata de personas y para la protección y asistencia a las víctimas de estos delitos, de la policía federal, y federal de telecomunicaciones, a cargo de Consuelo Argüelles Loya y suscrita por José Alejandro Montano Guzmán.
- 16 octubre 2014: Dictamen de las comisiones unidas de defensa nacional y estudios legislativos, a la minuta con proyecto de decreto por el que se reforman y adicionan diversas disposiciones de la ley orgánica del ejército y fuerza aérea mexicanos.
- 22 octubre 2015: Iniciativa con proyecto de decreto por el que se expide la Ley Federal para Prevenir y Sancionar los Delitos Informáticos, del senador Omar Fayad Meneses.
- 04 febrero 2016: Iniciativa con proyecto que reforma y adiciona diversas disposiciones del código penal federal, de la ley general de víctimas, de la ley de delitos de imprenta y del código nacional de procedimientos penales en materia de legislación regulatoria de los delitos informáticos contra niñas, niños y adolescentes, senadora Diva Hadamira Gastélum Bajo.
- 12 abril 2016: Iniciativa con proyecto de decreto por la que se reforman y adicionan diversas disposiciones del Código Penal Federal, la Ley de Sistema de Pagos, la Ley del Banco de México y de la Ley de Instituciones de Crédito, senadores, Ma. Del Rocío Pineda Gochi, Angélica del Rosario Araujo Lara, Lisbeth Hernández Lecona, Ivonne Liliana Álvarez García, Margarita Flores Sánchez y Óscar Román Rosas González.
- 19 abril 2016: Iniciativa con proyecto de decreto por el que se deroga el capítulo xi de la ley federal de protección de datos personales en posesión de particulares, denominado «de los delitos en materia del tratamiento indebido de datos personales», y se adiciona un título vigésimo séptimo al libro segundo del código penal federal, denominado «delitos contra la identidad de las personas», senador Arturo Zamora Jiménez.
- 28 abril 2016: De la comisión de justicia, con proyecto de decreto por el que se adiciona el artículo 430 del código penal federal, en materia de usurpación de identidad
- 06 septiembre 2016: Iniciativas con proyecto de decreto por el que se adiciona un capítulo III bis denominado robo de identidad, al título vigésimo segundo del código penal federal y se adiciona una fracción III al párrafo cuarto del artículo 115 de la ley de instituciones de crédito, senador René Juárez Cisneros.

- 13 octubre 2016: Iniciativa que adiciona diversas disposiciones del código penal federal, suscrita por la diputada Lorena Corona Valdés (PVEM) e integrantes del grupo parlamentario del PVEM].
- 21 julio 2017: Iniciativa con proyecto de decreto que reforma el código penal federal, presentada por el diputado Clemente Castañeda Hoeflich.
- 14 septiembre 2017: Iniciativa con proyecto de Decreto que adiciona al Título Decimoctavo el Capítulo III, artículo 287 Bis 287 Ter, del Código Penal Federal, DIP. Germán Ernesto Ralis Cumplido.
- 26 octubre 2017: Iniciativa con proyecto de decreto por el que reforma y adiciona diversas disposiciones del código penal federal, a cargo del diputado Roberto Alejandro Cañedo Jiménez.
- 30 octubre 2017: Iniciativa de ley con proyecto de decreto que adiciona la fracción III del artículo 139 del Código penal federal, a cargo de la senadora María Verónica Martínez Espinoza, Lisbeth Hernández Lecona y Ernesto Gándara Camou.
- 07 noviembre 2017: Iniciativa con proyecto de decreto por el que se reforman y adicionan diversas disposiciones del Código Penal Federal y del Código Nacional de Procedimientos Penales, en materia de delitos informáticos, evidencias digitales y medidas de cooperación internacional para combatir el ciberdelito, suscrita por la diputada Sofía González Torres e integrantes del grupo parlamentario del PVEM y el diputado Waldo Fernández González, del PRD.
- 06 marzo 2018: Que reforma y adiciona diversas disposiciones de la ley de la policía federal, del código nacional de procedimientos penales, del código penal federal y de la ley general para prevenir, sancionar y erradicar los delitos en materia de trata de personas y para la protección y asistencia a las víctimas de estos delitos, a cargo de la diputada Julieta Fernández Márquez.
- 17 abril 2018: Iniciativa que expide la ley general de seguridad privada, reforma diversas disposiciones de la ley general del sistema nacional de seguridad pública y abroga la ley federal de seguridad privada, a cargo del diputado César Alejandro Domínguez Domínguez.
- 15 noviembre 2018: Iniciativa que reforma y adiciona diversas disposiciones del código penal federal, a cargo del diputado Jorge Luis Preciado Rodríguez e integrantes del grupo parlamentario del PAN.
- 04 diciembre 2018: Iniciativa que reforma y adiciona diversas disposiciones al código penal federal, suscrita por el diputado Luis Alberto Mendoza Acevedo e integrantes del grupo parlamentario del PAN.
- 14 febrero 2019: Iniciativa con proyecto de decreto por el que se reforma el artículo 211 bis 1 del código penal federal, diputado José Salvador Rosas Quintanilla e integrantes del grupo parlamentario del PAN.
- 07 marzo 2019: Iniciativa que reforma el artículo 40 de la ley de puertos, suscrita por el diputado José Salvador Rosas Quintanilla e integrantes del grupo parlamentario del PAN.
- 19 marzo 2019: Iniciativa de la senadora Jesús Lucía Trasviña Waldenrath, con proyecto de decreto que reforma y deroga diversas disposiciones del

Título Noveno, Libro Segundo del Código Penal Federal y se expide la Ley de Seguridad Informática.

- 09 abril 2019: Iniciativa que reforma los artículos 14 de la ley orgánica de la fiscalía general de la república, 259 bis del código penal federal y 51 del código nacional de procedimientos penales, a cargo de la diputada Adriana Gabriela Medina Ortiz.
- 30 abril 2019: Iniciativa con proyecto de decreto para reformar y adicionar diversas disposiciones del código penal federal en materia de ciberseguridad, por la senadora Alejandra Lagunes Soto Ruiz.
- 31 julio 2019: Iniciativa con proyecto de decreto por el que se reforma el artículo 313 del código penal federal a fin de tipificar la inducción al suicidio por medio de redes sociales e informáticos.
- 03 septiembre 2019: Iniciativa que adiciona el artículo 140 bis al código penal federal, a cargo de la diputada Rocío Barrera Badillo.
- 10 septiembre 2019: Iniciativa que reforma y adiciona diversas disposiciones de la ley federal de protección de datos personales en posesión de los particulares, suscrita por la diputada Jacqueline Martínez Juárez e integrantes del grupo parlamentario del PAN.
- 12 septiembre 2019: Iniciativa con Proyecto de Decreto por el que se reforma el artículo 315, y el artículo 315 Bis del Código Penal Federal, senador Víctor Oswaldo Fuentes Solís.
- 12 septiembre 2019: Iniciativa con Proyecto de Decreto por el que se adiciona un inciso g) a la fracción I del artículo 10, de la Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro, Reglamentaria de la fracción XXI del artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, senador Víctor Oswaldo Fuentes Solís.
- 24 septiembre 2019: Iniciativa que reforma el artículo 73 de la constitución política de los estados unidos mexicanos, a cargo del diputado Javier Salinas Narváez.
- 15 octubre 2019: Iniciativa con proyecto de decreto para reformar y adicionar diversas disposiciones del código penal federal en materia de ciberdelito, Senadora Alejandra Lagunes Soto Ruiz.
- 23 octubre 2019: Dictamen proyecto de decreto por el que se adiciona una fracción VI al artículo 6 de la Ley General de Acceso a las mujeres a una vida libre de violencia[44].
- 05 febrero 2020: Iniciativa con proyecto de decreto por el que se reforman diversos artículos del código penal federal, en materia de adecuación constitucional, senador Miguel Ángel Mancera Espinoza.
- 05mMarzo 2020: Iniciativa del sen. Víctor Oswaldo Fuentes Solís, del grupo parlamentario del partido acción nacional, con proyecto de decreto por el que se adiciona un párrafo tercero al artículo 325 del Código Penal Federal.
- 01 septiembre 2020: Iniciativa con aval del grupo parlamentario que contiene proyecto de decreto por el que se modifica la denominación del capítulo II, del título noveno, del libro segundo y se reforma el artículo 211 bis 1 y se derogan diversos artículos del código penal federal; se reforman y adicionan diversos artículos de la ley general del sistema nacional de seguridad pública;

se adiciona una fracción XIV al artículo 5° de la ley de seguridad nacional; y se expide la Ley General de Ciberseguridad, Senador Miguel Ángel Mancera Espinosa.

Ya para finalizar, me gustaría destacar el trabajo de nuestra máxima casa de estudios la cual, a través de la Coordinación de Seguridad de la Información, emite bimestralmente la Revista Seguridad, la cual está especializada en la cultura de la prevención para TI.

En México, la brecha de desigualdad y la falta de infraestructura, hacen que apenas estemos tomando en consideración la parte de la ciberseguridad y protección de los datos personales; aún falta mucho, pero mucho camino por recorrer. La información que da forma a la mente, hay que cuidarla y aprenderla a trabajar, ya que tanto las "*fake news*" abundan en los medios digitales y podrían generar odios y rencores no necesarios por ver o creer cierta información. Ya lo decía Simón Wiesenthal: "La combinación de odio y tecnología es el mayor peligro que amenaza a la humanidad"[481].

[481] Frase vista en el Museo de Historia y Tolerancia.

Conclusiones

1. El sistema de la legislación de transparencia es un sistema complejo, ya que convergen tres subsistemas con naturaleza propia: El de transparencia y rendición de cuentas, el de datos personales, y el de archivos.

2. Por cuestiones prácticas, el sistema de datos personales se ha tenido que homologar en la aplicación de los principios, ya sea en los datos personales por sujetos obligados, o por los particulares.

3. En el camino de la construcción de estos nuevos derechos de vanguardia, las nuevas tecnologías avanzan a pasos agigantados y nos obligan a tratar de alcanzarla como mejor podemos, cuidando sobre todo a los usuarios finales para preservar su información y para dotarles de facilidades para ejercer sus derechos en lo particular, en lo general, así como estandarizar las obligaciones de las autoridades de transparentar sus recursos con el fin de fortalecer la democracia que cada vez está más golpeada por sus actores.

4. Ackerman tiene razón cuando indica que “no es ninguna coincidencia que la primera ley de acceso a la información fuera simultáneamente una ley que aseguraba la libertad de prensa. El acceso a la información gubernamental y la libertad de expresión se encuentran íntimamente conectados en tanto que los dos forman parte del concepto amplio de derecho a la información.”

5. El *big data* permite transformar en información muchos aspectos de la vida que antes no se podían cuantificar o estudiar, como los datos no estructurados.

6. El desarrollo tecnológico va más rápido que la legislación, el reto más grande lo representará el metaverso.

7. La información, está íntimamente aparejada con los datos personales; sin embargo, no siempre se tiene claro el matiz de la transparencia de la información, con la protección de los datos personales.

8. Hace falta mayor educación en el estudio del sistema de transparencia, datos personales y archivos.

9. El sistema de transparencia, es un sistema transversal que se une con otros sistemas, como el de seguridad, anticorrupción, ambiental, salud, entre otros, lo que hace un entramado y meta transversal de sistemas.

10. La clasificación de la información puede generar problemas de opacidad disfrazada, pero también podrían clasificarse indiscriminadamente determinada información, que algún sujeto obligado considere de interés público o interés nacional.

11. Ahora se podría gestar una opacidad positiva; es decir, el hecho de colocar tanta información en las páginas gubernamentales, se podría ocultar información a plena vista. Dicho en otras palabras, para encontrar información, podría ser buscar una aguja en un pajar.

12. El futuro de la protección de los datos de las personas morales que se equiparen a datos personales, aun es incierto; considero que también se deben proteger de la misma forma que una persona física, pero por nuestro sistema, serán los tribunales lo que marcarán tendencia.

13. La ciberseguridad cada vez tendrá más importancia, se deberán modificar las leyes penales, para ver las modernas conductas delictivas.

14. Las acreditaciones ante el INAI como en el caso de la autorregulación vinculante, irán tomando mayor preocupación en los sujetos regulados, quienes deberán mejorar tanto la forma del cuidado del tratamiento de los datos personales, como de las medidas de seguridad, técnicas, físicas y administrativas.

15. Se deberá tener mucho cuidado con la cancelación de los datos personales, para no tener problemas con el llamado derecho al olvido.

Bibliografía

Ackerman M., John y Sandoval, Irma E., *Leyes de acceso a la información en el mundo*, [en línea] México, Cuadernos de Transparencia, Número 7, INAI, 2015, *https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/Cuadernillo%2007.pdf*

Ackerman, Jhon M., *Organismos Autónomos y la nueva división de poderes en México y América Latina*, en "Homenaje al Doctor Emilio O. Rabasa", [en línea], México, IIJ-UNAM, 2016, *https://archivos.juridicas.unam.mx/www/bjv/libros/6/2834/5.pdf*

Barnard, Alicia, *et. al*. *Breviario de Metadatos*, [en línea], México, AGN, Serie: Temas fundamentales de preservación digital, 2016, *https://www.gob.mx/cms/uploads/attachment/file/228991/InterPARES_4_020617.pdf*

Chul Han, Byung, La sociedad de la transparencia, España, Herder, 2013.

Clímaco Valiente, Ernesto, *Génesis histórico-normativa del derecho a la protección de los datos personales desde el derecho comparado a propósito de su fundamento*, [en línea] España, Universidad Carlo III de Madrid, 2012, *https://e-archivo.uc3m.es/bitstream/handle/10016/18785/TFM_MEADH_Ernesto_Climaco.pdf?sequence=1&isAllowed=y*

Fuenmayor E. Alejandro, *El derecho de acceso de los Ciudadanos a la Información Pública*, [en línea] Costa Rica, UNESCO, 2004, *https://www.iidh.ed.cr/derecho-informacion/media/1077/acceso_informacion_desarrollos_otros_unesco_propuesta_ley_modelo.pdf*

Gilliland-Swetland, Anne, *La definición de los metadatos*, en Getty Trust, J. Paul Coord. "Introducción a los Metadatos. Vías a la información digital", [en línea] USA, 1999, *http://d2aohiyo3d3idm.cloudfront.net/publications/virtuallibrary/0892365358.pdf*

Guerrero Gutiérrez, Eduardo, *La luz en busca del cristal hacia la transparencia y la rendición de cuentas en México*, en "Ensayos cultura de transparencia y rendición de cuentas en la gestión pública", [en línea], México, IFE, 2003, *https://educacion.michoacan.gob.mx/wp-content/uploads/2015/03/culturatransparenciaddd.pdf*

INAI, *Introducción y antecedentes del Derecho a la Protección de Datos Personales*, [en línea] México, INAI, 2015 *http://metabase.uaem.mx/xmlui/bitstream/handle/123456789/2523/1%20Introducci o%CC%81n%20y%20antecedentes%20del%20Derecho%20a%20la%20Proteccio*

%CC%81n%20de%20Datos%20Personales.pdf?sequence=1&isAllowed=y

INAI, *Reforma al artículo 6° constitucional que establece el acceso a la información pública como un derecho fundamental de los mexicanos*, México, INAI, 2007, *https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/ModificacionArt6.pdf*

López Sabater, Verónica, (coord.) *Economía de los Datos, Riqueza 4.0*, España, Ariel, 2017.

Luhmann, Niklas, *Sistemas sociales, Lineamientos para una teoría general*, México, Universidad Iberoamericana, 2da ed, 1998.

Martínez Becerril, Rigoberto, *El derecho de Acceso a la Información en México, su ejercicio y medios de impugnación*, [en línea] México, INFOEM, 2009, *https://www.infoem.org.mx/sipoem/ipo_capacitacionComunicacion/pdf/pet_tesis_001_2008.pdf*

Martínez Bejarano, María Eugenia *Coord*, *Compilación Jurídica de los otros sujetos obligados por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental*, [en línea] México, IIJ-INAI, 2005, *https://biblio.juridicas.unam.mx/bjv/detalle-libro/5181-compilacion-juridica-de-los-otros-sujetos-obligados-por-la-ley-federal-de-transparencia-y-acceso-a-la-informacion-publica-gubernamental*

Muñoz de Alba Medrano, Marcia, *Habeas Data*, en "Documentos de trabajo del Instituto de Investigaciones Jurídicas. 2001", [en línea] México, UNAM-IIJ, 2001, https://archivos.juridicas.unam.mx/www/bjv/libros/10/4643/11.pdf

Navarro, Erick, *De los mecanismos de participación ciudadana a la consolidación de gobierno abierto*, en Naser Alejandra (Coord), "Gobierno abierto y ciudadanía en el centro de la gestión pública", [en línea], CEPAL, ONU, 2021, *https://repositorio.cepal.org/bitstream/handle/11362/47256/1/S2100371_es.pdf*

Pulido Zaballos, Emilia, *La Protección de Datos Personales en España: Evolución Normativa y Criterios de Aplicación*, [en línea], España, Universidad Complutense de Madrid, 2013, *https://eprints.ucm.es/22849/1/T34733.pdf*

Sagüés, Néstor Pedro, *El Habeas Data: Su desarrollo constitucional*, en "V Congreso Iberoamericano de derecho constitucional", [en línea] México, Estudios Doctrinales, Serie G., número 193, UNAM-IIJ, 1998, *https://archivos.juridicas.unam.mx/www/bjv/libros/1/113/39.pdf* p. 859.

Salas Juárez, Joel, *El papel de los órganos garantes del acceso a la información pública en el contexto del Estado Abierto*, en "Desde el gobierno abierto al Estado abierto en América Latina y el Caribe", [en línea] Chile, CEPAL, 2017,

https://archivos.juridicas.unam.mx/www/bjv/libros/10/4686/28.pdf p. 152.

Solís García, Bertha, "Evolución de los Derechos Humanos", en Moreno Bonett, Margarita y Álvarez de Lara, Rosa María, *El Estado laico y los derechos humanos en México: 1810-2010*, [en línea] México, UNAM, Instituto de Investigaciones Jurídicas, Tomo I, 2012.
https://archivos.juridicas.unam.mx/www/bjv/libros/7/3100/9.pdf

Soto Gama, Daniel, *Principios Generales del Derecho a la Información*, [en línea] México, INFOEM, 2010,
https://www.infoem.org.mx/sipoem/ipo_capacitacionComunicacion/pdf/pet_tesis_003_2009.pdf

Tascón Mario, Coullaut Arantza, *Big Data y el Internet de las cosas, Qué hay detrás y cómo nos va a cambiar*, España, Catarata, 2016.

Téllez Valdés, Julio, *Derecho Informático*, 2ª ed., México, McGraw-Hill, 1996, p. 22.

Torres Nafarrete (*sic*), Javier, *Introducción a la Teoría de Sistemas de Niklas Luhmann*, [en línea] México, UNAM, Colección Aprender a Aprender, Serie Perspectivas en la Teoría de Sistemas, 1999,
http://computo.ceiich.unam.mx/webceiich/docs/libro/Introduccion_a_la_teoria_de_sistemas_de_Niklas_Luhmann.pdf

Trejo Delarbre, Raúl *et. al. Democracia, acceso a la información y tecnología*, en "Transparencia y acceso a la información, las tendencias en el mundo", [en línea] México, IIJ-UNAM, 2005,
https://archivos.juridicas.unam.mx/www/bjv/libros/6/2503/3.pdf

UNESCO, *Actas de la Conferencia General*, París, UNESCO, 38ª reunión, Vol 1. Resoluciones, 2016, *https://unesdoc.unesco.org/ark:/48223/pf0000243325_spa*

UNESCO, *Leyes de acceso a la información*, [en línea] UNESCO, s.d. Disponible en: *https://es.unesco.org/themes/leyes-acceso-informacion*

Valenzuela Mendoza, Rafael Enrique y Bojórquez Pereznieto, José Antonio, *Modelos de implementación del Gobierno Abierto en México*, en "Gobierno Abierto y el Valor de la información pública", [en línea] México, UNAM-IIJ, 2016,
https://archivos.juridicas.unam.mx/www/bjv/libros/9/4016/9.pdf p. 134.

Von Bertalanffy, Ludwig, *Teoría General de los Sistemas*, México, FCE, 1986.

Hemerografía

Javier Acuña, Francisco, "*¿Información es poder? No, puede ser mucho más útil*", El Financiero, Secc. Opinión, México, junio, 2020, *https://www.elfinanciero.com.mx/opinion/francisco-javier-acuna/informacion-es-poder-no-puede-ser-mucho-mas-util*

Revistas

Armitage, David y Guldi, Jo, "Grandes Problemas: Los Big Data", *Revista Cultural de Santander*, Núm. 12, España, Sección Nuevas Corrientes Intelectuales, Universidad Industrial de Santander, 2017 [*https://revistas.uis.edu.co/index.php/revistasantander/article/download/8909/8794/*

Castells, Manuel, citado por Aldana Rendón, Mario, "Reseña de" *Castells: la era de la información. Realizades y reflexiones sobre la globalización*, [en línea], México, Espiral, vol. VI, no. 18, 2000, Redalyc, *https://www.redalyc.org/articulo.oa?id=13861811* p.286

Dermizaky Peredo, Pablo, "El Derecho a la intimidad", *Ius et Praxis*,[en línea] Chile, Universidad de Talca, Vol. 6. No. 1, 2000, *https://www.redalyc.org/pdf/197/19760113.pdf*

Fernández Ruiz, Jorge, *Apuntes para una Teoría Jurídica de las Actividades del Estado*, [en línea], México, IIJ-UNAM, Boletín Mexicano de Derecho Comparado No. 99, septiembre – diciembre 2000, *http://historico.juridicas.unam.mx/publica/rev/boletin/cont/99/art/art1.htm*

García González, Aristeo, "La Protección de Datos Personales: Derecho Fundamental del Siglo XXI. Un Estudio Comparado" en *Boletín Mexicano de Derecho Comparado*, [en línea] Número 120, México, UNAM, Instituto de Investigaciones Jurídicas, 2007. *https://revistas.juridicas.unam.mx/index.php/derecho-comparado/article/view/3933/4971*

Mayorga-Jácome, Tannia C. *et. al*. "Historia de la normativa reguladora de la Protección de Datos de Carácter personal en distintos países Latinoamericanos" en *Revista Dominio de las Ciencias*, México, Vol. 5, núm. 1., enero 2019, *https://dominiodelasciencias.com/ojs/index.php/es/article/view/875/pdf*

Martínez Luna, Gilberto Lorenzo, "Minería de Datos: cómo hallar una aguja en un pajar", *Revista Ciencia*, [en línea] Vol. 62, No. 3. Julio-septiembre 2011, CONACYT-Academia Mexicana de Ciencias, *https://www.revistaciencia.amc.edu.mx/images/revista/62_3/PDF/mineria_aguja.pd*

f

Maté Jiménez, Carlos, "*Big Data*. Un nuevo paradigma de análisis de datos", *Revista Anales de mecánica y electricidad*, Universidad Pontificia Comillas, España, noviembre-diciembre 2014, en: *https://www.iit.comillas.edu/docs/IIT-14-153A.pdf*

Morales Tostado, María del Carmen, *Participación de la sociedad civil en el derecho de acceso a la información pública*, en BIOLEX, Revista Jurídica del Departamento de Derecho de la Universidad de Sonora, [en línea] México, Vol. 12, No. 22, enero-junio 2020, *https://biolex.unison.mx/index.php/biolex_unison_mx/issue/view/23/31*

Nieves Saldaña, María, *«The Right to Privacy» La génesis de la Protección de la Privacidad en el sistema constitucional norteamericano: El centenario legado de Warren y Brandeis*, España, Revista de Derecho Político, No. 85, 2012, *https://doi.org/10.5944/rdp.85.2012.10723*

Origgi, Gloria, "*Terminó la era de la información, ahora todo es reputación*" Revista Letras Libres, México, 03 de mayo de 2018, *https://www.letraslibres.com/espana-mexico/revista/termino-la-era-la-informacion-ahora-todo-es-reputacion*

Osorio, Francisco, *et. al. La Nueva Teoría Social en Hispanoamérica. Introducción a la Teoría de sistemas Constructivista*, [en línea] México, UAEMex, Colección Pensamiento Universitario, Número 11, 2008. *http://ri.uaemex.mx/bitstream/handle/20.500.11799/3617/Nueva_teoria_social_en_Hispanoamerica_Osorio_Arnold.pdf?sequence=3*

Quirós Camacho, Jenny, *La Protección de Datos Personales y el habeas data. Elementos para iniciar una discusión en Costa Rica*, en "Revista de Ciencias Jurídicas", Costa Rica, Portal de Revistas Académicas, número 103, 2004, *https://revistas.ucr.ac.cr/index.php/juridicas/article/download/13370/14345/*

Riquelme, José C.; Ruiz, Roberto; Gilbert, Karina, "Minería de Datos: Conceptos y Tendencias", Inteligencia Artificial. [en línea] Revista Iberoamericana de Inteligencia Artificial, vol. 10, núm. 29, primavera, España, 2006, *https://www.redalyc.org/pdf/925/92502902.pdf*

Senso, José A. y de la rosa Piñeiro, Antonio, *El concepto de metadato. Algo más que descripción de recursos electrónicos*, [en línea] Brasil, Revista Scielo, v. 32, n. 2, may-ago 2003, *https://www.scielo.br/j/ci/a/ZHtZZfYnJfKqVn4tGNSw4yv/?format=pdf&lang=es*

Diccionarios

El Economista, *Diccionario de Economía*, [en línea] El economista.es, España, s/d., *https://www.eleconomista.es/diccionario-de-economia/*

Real Academia Española, *Diccionario de la Real Academia Española*, 2021, *https://dle.rae.es*

Wikipedia. *Wikipedia, La enciclopedia libre*, 2022, *https://es.wikipedia.org*

Documentos Diversos

Agencia Española de Protección de Datos, *Directrices sobre los delegados de datos (DPD)*, [en línea], España, AEPD, Grupo de Trabajo sobre Protección de Datos del Artículo 29, 2017, *https://www.aepd.es/sites/default/files/2019-09/wp243rev01-es.pdf*

Agencia Española de Protección de Datos, *Guía del Reglamento General de Protección de Datos para Responsables de tratamiento*, [en línea], España, AEGP, 22 de mayo de 2018, *https://www.aepd.es/sites/default/files/2019-12/guia-rgpd-para-responsables-de-tratamiento.pdf*

AGN, *Breviario de metadatos*, [en línea] México, AGN, Serie: Temas fundamentales de preservación digital, no. 4, 2016,

https://www.gob.mx/cms/uploads/attachment/file/228991/InterPARES_4_020617.pdf

Aguilar, José, *Introducción a la Minería de Datos, Metodologías y Técnicas de Minería de Datos*, Venezuela, Universidad de los Andes, *http://www.ing.ula.ve/~aguilar/actividad-docente/IN/transparencias/clase40.pdf*

Beltrán Martínez, Beatriz, "*Minería de Datos*", México, BUAP, *http://bbeltran.cs.buap.mx/NotasMD.pdf*

Castells, Manuel, La era de la información. Economía, sociedad y cultura. Vol. 1 México, siglo XXI, 1996, *http://www.economia.unam.mx/lecturas/inae3/castellsm.pdf*

Comisión Europea, *El espacio Schengen, La Europa sin fronteras*, Comisión Europea, 2015, *https://op.europa.eu/en/publication-detail/-/publication/09fcf41f-ffc4-472a-a573-b46f0b34119e/language-es*

Cruz Revueltas, Juan Cristóbal, *Moral y transparencia. Fundamento e implicaciones morales de la transparencia*, [en línea] Cuadernos de Transparencia, México, INAI, 2015, *https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/Cuadernillo%2015%20B.pdf*

De Jesús Lozano Ocman, Magda Eugenia, *Propuesta de Plan de Trabajo 2021-2022 para la Coordinación de la Comisión de Tecnologías de la Información y Plataforma Nacional de Transparencia*, [en línea] México, SNT-INAI, 2021, *https://snt.org.mx/wp-content/uploads/2022/01/MEJLO_TIyPNT_2022.pdf*

Gamboa Montejano, Claudia, *Transparencia y Acceso a la Información Pública. Estudio de Antecedentes, Marco Jurídico Actual, Derecho Comparado de Diversos Países y de las Entidades Federativas, y de las iniciativas Presentadas en el Tema*, [en línea] México, CDDHCU. 2007, *http://www.diputados.gob.mx/sedia/sia/spi/SPI-ISS-03-07.pdf*

Gobierno de la República [México], *Reforma en Materia de Transparencia*, [en línea], México, Gobierno de la República, 2014, *https://www.gob.mx/cms/uploads/attachment/file/66464/13_Transparencia.pdf*

Hirwade, Anil y Hirwade Mangala, "*Metadata Harvesting Service in India*", [en línea], EUA, en Library Herald, 2006, vol. 44, n. 4, *http://eprints.rclis.org/9295/*

INAI, *El ABC del Gobierno Abierto,* [en línea], México, INAI, 2020, *https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/digital_el_abc.pdf*

INAI, *Introducción a la Ley Federal de Transparencia y Acceso a la Información Pública. Manual del Participante*, [en línea], México, INAI, 2016, [*https://www.sep.gob.mx/work/models/sep1/Resource/18094/4/images/m_ilftaip.pdf*

INAI, *Gobierno Abierto y Transparencia Proactiva. Manual del Participante*, [en línea] México, INAI, 2017, *https://transparencia.info.jalisco.gob.mx/sites/default/files/manualgaimprenta.pdf*

INAI, *Políticas de Gobierno Abierto y Transparencia Proactiva*, [en línea], México, SNT-INAI, s.a., *https://gobiernoabiertogto.org.mx/documentos/libros/46.pdf*

Naser, Alejandra, y Ramírez Alujas, Álvaro, *Plan de Gobierno Abierto, Una hoja de ruta para los Gobiernos de la región*, [en línea], Chile, CEPAL, Serie Manuales, 2017, *https://repositorio.cepal.org/bitstream/handle/11362/36665/4/S1700687_es.pdf*

Organización para la Cooperación y el Desarrollo Económicos, *Gobierno Abierto, Contexto mundial y el camino a seguir, aspectos claves 2016,* [en línea] EUA,

OCDE, 2016, *https://www.oecd.org/gov/Open-Government-Highlights-ESP.pdf*

ONU, *El derecho a la privacidad en la era digital*, A/C.3/71/L.39 de fecha 31 de octubre de 2016, [en línea] Asamblea General - UN Digital Library, 2016, *https://digitallibrary.un.org › A_C-3_71_L-39-ES*

ONU, *Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión*, acuerdo A/HRC/23/40 de fecha 17 de abril de 2013 [en línea] Asamblea General - UN Digital Library, 2013, *https://undocs.org/es/A/HRC/23/40*

Pérez Haydeé y Terrazas Renata, *Acceso a la Información y transparencia en México*, Razones FUNDAR, México, s.d, *https://www.fundar.org.mx/mexico/pdf/transparencyacceso.pdf*

Rodríguez Zepeda, Jesús, *Estado y Transparencia: Un paseo por la filosofía política*, [en línea] Cuadernos de Transparencia, México, Número 4, INAI. 2015, *https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/Cuadernillo%2004%20B.pdf*

Rodríguez Zepeda, Jesús, *Sensibilización para la transparencia y rendición de cuentas. Manual del Participante* [en línea] México, INAI, 2015. *https://www.sep.gob.mx/work/models/sep1/Resource/18094/4/images/m-sensibilizacion.pdf*

UNAM, *Lineamientos para la Integración de Repositorios Universitarios en el Repositorio Institucional de la UNAM,* [en línea] México, en “Gaceta UNAM” Número 5,156, 19 de octubre de 2020, *https://www.gaceta.unam.mx/wp-content/uploads/2020/10/201019.pdf*

Páginas de Internet

Bautista Villagómez, Diana, *Big Data: El poder de la información*, México, IEXE, Universidad en línea, 2018, *https://www.iexe.edu.mx/ciencia-y-tecnologia-blog/big-data-el-poder-de-la-informacion.html*

Bello, Elena, *Big Data: qué es, para qué sirve y por qué es importante*,[en línea] España, IEB SCHOOL, Blog, 15 de octubre de 2021, *https://www.iebschool.com/blog/valor-big-data/*

BBVA, *Una de cada dos empresas reconoce que no sabe obtener valor de los datos*, España, BBVA on line, secc. Big Data, 18 de agosto de 2017, *https://www.bbva.com/es/dos-empresas-reconoce-sabe-obtener-valor-datos/*

BBVA, *La era de la información: cinco claves de su futuro*, [en línea] España, BBVA, secc. Innovación, 11 de agosto de 2017, *https://www.bbva.com/es/informacion-cinco-claves-futuro/*

Cámara de Senadores, *Iniciativa con proyecto de decreto por la que se expide la ley general de protección de datos personales en posesión de sujetos obligados*, [en línea] s.d. *https://www.senado.gob.mx/comisiones/gobernacion/docs/proteccion_datos/Iniciativa.pdf*

Chen, Caterina, "*El conocimiento es poder*", Cultura Genial, Frases y Discursos, *https://www.culturagenial.com/es/el-conocimiento-es-poder/#:~:text=%22El%20conocimiento%20es%20poder%22%20significa,o%20alguien%2C%20m%C3%A1s%20poder%20tendr%C3%A1.&text=Francis%20Bacon%20(1561%2D1626)%3A,para%20promover%20la%20ciencia%20aplicada.*

Comité Europeo de Protección de Datos, *Grupo de Trabajo del artículo 29*, EDPB (*European Data Protection Board*), s/d, *https://edpb.europa.eu/our-work-tools/article-29-working-party_es*

D. Ruben, Brent, "*En la era de la información: información, tecnología y estudio del comportamiento*", EUA, Rutgers University, 1990, *En la era de la información: información, tecnología y estudio ...revistas.ucm.es › index.php › DCIN › article › download*,

Dirección General de Repositorios Universitarios, *Estándar de Datos de Objetos Digitales Dublin Core Cualificados (DC)*, [en línea] México, UNAM, octubre 2019, *https://dgru.unam.mx/wp-content/uploads/2019/10/D.ST_.DGRU_CDI_009_2015_C_OD_Dublin_Core.pdf*

Dublin Core, *About DCMI, s/d,* [en línea] *https://www.dublincore.org/about/*

Dublin Core, *DCMI Metadata Terms*, 2020, *http://dublincore.org/specifications/dublin-core/dcmi-terms/2020-01-20/*

Galimany Suriol, Aleix y Bachs Ferrer, Jordi, *La creación de valor en las empresas a través del Big Data*, España, *Universitat* de Barcelona, 2014, *http://diposit.ub.edu/dspace/bitstream/2445/67546/1/TFG-ADE-Galimany-Aleix-juliol15*.pdf

Guerrero López, Jorge y Rodríguez Pinilla, Jorge Eduardo, "Diseño y Desarrollo de una Guía para la implementación de un ambiente Big Data en la Universidad Católica de Colombia", Universidad Católica de Colombia, 2013, Colombia, https://repository.ucatolica.edu.co/bitstream/10983/1320/1/DISE%C3%91O%20Y%

20DESARROLLO%20DE%20UNA%20GU%C3%8DA%20PARA%20LA%20IMPLEMENTACI%C3%93N%20DE%20UN%20AMBIENTE%20BIG%20DATA%20EN%20LA%20UNIVERSIDAD%20CAT%C3%93LICA%20DE%20COLOMBIA.pdf

Instituto Gallego de Promoción Económica, *Oportunidades Industria 4.0 en Galicia*, Junta de Galicia, España, 2017, [fecha de consulta: 3 de diciembre de 2022] Disponible en: *http://www.igape.es/gl/ser-mais-competitivo/galiciaindustria4-0/estudos-e-informes/item/download/68_b27b22a11c4f195d9d8888e875e77358*

Martínez Alpañez, Rubén, "*La información es poder*", La opinión de Murcia, Opinión, España, Espacio Abierto, 2014, *https://www.laopiniondemurcia.es/opinion/2014/03/27/informacion/546861.html*

Ribas, Ester, "¿Qué es el Data Mining o minería de datos?", España, IEBS, 2018, [https://w*ww.iebschool.com/blog/data-mining-mineria-datos-big-data/*

s/a, "*¿Qué es la minería de datos?*" Kaspersky, s.d, *https://latam.kaspersky.com/resource-center/definitions/data-mining*

UNAM, Introducción a la minería de Datos, México, UNAM, enero 2020, https://docencia.tic.unam.mx/presenciales/Introduccion-a-la-mineria-de-datos.html

Yebra Serrano, Irene, *Día internacional de la protección de datos; 28 de enero*, España, INEAF Business School¸ 28 de enero de 2019, *https://www.ineaf.es/tribuna/dia-internacional-de-la-proteccion-de-datos-28-de-enero/*

Zapata, Enrique, *La diferencia entre Datos Abiertos y Gobierno Abierto*, [en línea], México, Datos Abiertos México, 17 de abril de 2018, *https://datos.gob.mx/blog/la-diferencia-entre-datos-abiertos-y-gobierno-abierto*

Tesis del Semanario Judicial de la Federación

ACCESO A LA INFORMACIÓN. IMPLICACIÓN DEL PRINCIPIO DE MÁXIMA PUBLICIDAD EN EL DERECHO FUNDAMENTAL RELATIVO. Tesis: I.4o.A.40 A (10a.), Semanario Judicial de la Federación y su Gaceta, Décima Época, t. III, marzo de 2013, p. 1899.

ACCESO A LA INFORMACIÓN. LAS NORMAS PENALES NO PUEDEN RESTRINGIR EL GOCE DEL NÚCLEO ESENCIAL DE ESTE DERECHO. Tesis: 1a. CCCXCIX/2015 (10a.) Gaceta del Semanario Judicial de la Federación, Décima Época, t. I, diciembre de 2015, p. 253.

ACCESO A LA INFORMACIÓN. SU NATURALEZA COMO GARANTÍAS

INDIVIDUAL Y SOCIAL. Tesis P./J. 54/2008, Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XXVII, junio de 2008, p. 743.

COMPETENCIA POR MATERIA PARA CONOCER DEL AMPARO PROMOVIDO CONTRA LA RESPUESTA DEL TITULAR DE LA UNIDAD ESPECIALIZADA DE TRANSPARENCIA Y APERTURA GUBERNAMENTAL DE LA PROCURADURÍA GENERAL DE LA REPÚBLICA A UNA SOLICITUD DE ACCESO A LA INFORMACIÓN RELACIONADA CON UNA INVESTIGACIÓN CRIMINAL, AVERIGUACIÓN PREVIA O CARPETA DE INVESTIGACIÓN. SI LA CONTESTACIÓN CONTIENE LA INTERPRETACIÓN DE NORMAS PENALES, CORRESPONDE A UN JUZGADO DE DISTRITO DE AMPARO EN MATERIA PENAL. Tesis: I.6o.P.130 P (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. II, diciembre de 2018, p. 1071.

COPIA CERTIFICADA DE UN EXPEDIENTE CLÍNICO. CUANDO SE SOLICITA EN EJERCICIO DEL DERECHO DE ACCESO A LA INFORMACIÓN, LA AUTORIDAD QUE SE PRONUNCIE EN RELACIÓN CON EL COSTO DE SU EXPEDICIÓN, EN OBSERVANCIA AL PRINCIPIO PRO PERSONA, NO DEBE APLICAR EL ARTÍCULO 83, FRACCIÓN I, DE LA LEY DE INGRESOS DEL ESTADO DE PUEBLA, PARA EL EJERCICIO FISCAL 2015, QUE PREVÉ LA CUOTA APLICABLE POR LA CERTIFICACIÓN DE DATOS O DOCUMENTOS. Tesis: VI.2o.A.11 A (10a.) Gaceta del Semanario Judicial de la Federación, t. IV, octubre de 2016, p. 2852.

DERECHO A LA INFORMACIÓN. LA SUPREMA CORTE INTERPRETÓ ORIGINALMENTE EL ARTÍCULO 6o. CONSTITUCIONAL COMO GARANTÍA DE PARTIDOS POLÍTICOS, AMPLIANDO POSTERIORMENTE ESE CONCEPTO A GARANTÍA INDIVIDUAL Y A OBLIGACIÓN DEL ESTADO A INFORMAR VERAZMENTE. Tesis: P. XLV/2000, Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo XI, abril de 2000, p. 72.

DERECHO A LA INFORMACIÓN. GARANTÍAS DEL. Tesis: 2a. LXXXV/2016 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. I, septiembre de 2016, p. 839.

DERECHO A LA INFORMACIÓN. NO DEBE REBASAR LOS LÍMITES PREVISTOS POR LOS ARTÍCULOS 6o., 7o. Y 24 CONSTITUCIONALES. Tesis: I.3o.C.244 C, Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XIV, septiembre de 2001, p. 1309.

DERECHO A LA INFORMACIÓN. SU EJERCICIO SE ENCUENTRA LIMITADO TANTO POR LOS INTERESES NACIONALES Y DE LA SOCIEDAD, COMO POR LOS DERECHOS DE TERCEROS. Tesis: P. LX/2000, Semanario Judicial de la Federación y su Gaceta, t. XI, abril de 2000, p. 74.

DERECHO A LA INFORMACIÓN PÚBLICA. EVOLUCIÓN CONSTITUCIONAL DE

LA REGULACIÓN DE ESA PRERROGATIVA. Tesis: I.15o.A.118 A, Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XXIX, abril de 2009, p. 1880.

DERECHOS AL HONOR, A LA INTIMIDAD Y A LA PROPIA IMAGEN. CONSTITUYEN DERECHOS HUMANOS QUE SE PROTEGEN A TRAVÉS DEL ACTUAL MARCO CONSTITUCIONAL. Tesis: I.5o.C.4 K (10a.), Semanario Judicial de la Federación y su Gaceta, Décima Época, Tomo 2, junio de 2013, p. 1258.

FACULTADES DEL INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES (INAI). LAS EJERCIDAS AL IMPONER SANCIONES ECONÓMICAS, DERIVADO DE LA DENUNCIA PRESENTADA POR UN PARTICULAR, SON REGLADAS Y NO DISCRECIONALES. Tesis: I.4o.A.211 A (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. III, febrero de 2021, p. 2867.

FEDERACIONES DEPORTIVAS MEXICANAS. SON SUJETOS DE FISCALIZACIÓN Y QUEDAN VINCULADAS POR LOS DERECHOS A LA LIBERTAD DE EXPRESIÓN Y DE ACCESO A LA INFORMACIÓN.

FLUJO DE INFORMACIÓN EN RED ELECTRÓNICA (INTERNET). PRINCIPIO DE RESTRICCIÓN MÍNIMA POSIBLE. Tesis: 2a. CII/2017 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. II, junio de 2017, p. 1433. Tesis: PC.I.A. 2 A (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. III, agosto de 2016, p. 2253.

GARANTIAS INDIVIDUALES (DERECHO A LA INFORMACION). VIOLACION GRAVE PREVISTA EN EL SEGUNDO PARRAFO DEL ARTICULO 97 CONSTITUCIONAL. LA CONFIGURA EL INTENTO DE LOGRAR LA IMPUNIDAD DE LAS AUTORIDADES QUE ACTUAN DENTRO DE UNA CULTURA DEL ENGAÑO, DE LA MAQUINACION Y DEL OCULTAMIENTO, POR INFRINGIR EL ARTICULO 6o. TAMBIEN CONSTITUCIONAL. Tesis: P. LXXXIX/96, Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo III, junio de 1996, p. 513.

INFORMACION. DERECHO A LA, ESTABLECIDO POR EL ARTICULO 6o. DE LA CONSTITUCION FEDERAL. Tesis: 2a. I/92, Semanario Judicial de la Federación, Octava Época, Tomo X, agosto de 1992, página 44.

INFORMACIÓN PÚBLICA. ES AQUELLA QUE SE ENCUENTRA EN POSESIÓN DE CUALQUIER AUTORIDAD, ENTIDAD, ÓRGANO Y ORGANISMO FEDERAL, ESTATAL Y MUNICIPAL, SIEMPRE QUE SE HAYA OBTENIDO POR CAUSA DEL EJERCICIO DE FUNCIONES DE DERECHO PÚBLICO. Tesis: 2a. LXXXVIII/2010, Semanario Judicial de la Federación y su Gaceta Registro, Novena Época, t. XXXII, agosto de 2010, p. 463.

JUICIO CONTENCIOSO ADMINISTRATIVO FEDERAL. ES IMPROCEDENTE CONTRA LAS RESOLUCIONES EMITIDAS POR EL INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES (INAI), EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE PARTICULARES. Tesis: 2a./J. 31/2020 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. I, octubre de 2020, p. 668.

LIBERTAD DE EXPRESIÓN Y DERECHO A LA INFORMACIÓN. SU IMPORTANCIA EN UNA DEMOCRACIA CONSTITUCIONAL. Tesis 1a. CCXV/2009, Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XXX, diciembre de 2009, p. 287.

PLAN TÉCNICO FUNDAMENTAL DE INTERCONEXIÓN E INTEROPERABILIDAD, PUBLICADO EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 10 DE FEBRERO DE 2009. SUS ARTÍCULOS 3, 5, 8, 10, 15, 24, 28 Y 34, NO VIOLAN EL PRINCIPIO DE DISTRIBUCIÓN DE COMPETENCIAS ESPECIALIZADAS EN LA ADMINISTRACIÓN PÚBLICA FEDERAL, NI PROVOCAN UNA DOBLE REGULACIÓN EN MATERIA DE ACCESO A LA INFORMACIÓN. Tesis: I.1o.A.E.135 A (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. IV, mayo de 2016, p. 2830.

PROTECCIÓN DE DATOS PERSONALES. CONSTITUYE UN DERECHO VINCULADO CON LA SALVAGUARDA DE OTROS DERECHOS FUNDAMENTALES INHERENTES AL SER HUMANO. Tesis: I.10o.A.5 CS (10a.), Semanario Judicial de la Federación, Décima Época, Tomo III, Septiembre de 2019, p. 2199.

PRUEBA DOCUMENTAL EN EL JUICIO DE AMPARO. EN TÉRMINOS DEL ARTÍCULO 121 DE LA LEY DE AMPARO, EL SERVIDOR PÚBLICO QUE POSEA ALGÚN DOCUMENTO OFRECIDO Y ADMITIDO COMO TAL NO PUEDE REHUSARSE A UN REQUERIMIENTO JUDICIAL, SOBRE LA BASE DE QUE DEBE ESTARSE A LO RESUELTO EN UN PROCEDIMIENTO DE ACCESO A LA INFORMACIÓN. Tesis: P./J. 13/2018 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. I, junio de 2018, p. 12.

PRUEBAS EN EL AMPARO INDIRECTO. NO EXISTE OBLIGACIÓN DEL JUZGADOR DE REQUERIR LAS COPIAS O DOCUMENTOS OFRECIDOS Y SOLICITADOS EN TÉRMINOS DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA A UNA UNIDAD DE ENLACE O UNIDAD DE TRANSPARENCIA, AUN CUANDO EN LA PETICIÓN SE HAYA INVOCADO EL ARTÍCULO 121 DE LA LEY DE AMPARO. Tesis: I.1o.A.E.42 K (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. IV, enero de 2016, p. 3397.

PRUEBAS EN EL JUICIO DE AMPARO INDIRECTO. SI UNA DE LAS PARTES OFRECE COPIAS O DOCUMENTOS EN PODER DE UNA AUTORIDAD, LOS

CUALES SOLICITÓ SIN QUE SE EXPIDIERAN, EL JUEZ DE DISTRITO, DE CONFORMIDAD CON EL ARTÍCULO 121 DE LA LEY DE LA MATERIA, DEBE REQUERÍRSELOS, AUN CUANDO LA PETICIÓN A ESA AUTORIDAD SE HAYA EFECTUADO A TRAVÉS DE SU UNIDAD DE ENLACE O DE TRANSPARENCIA, EN TÉRMINOS DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. Tesis: III.5o.A.3 K (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. IV, septiembre de 2016, p. 2890.

PUEBLOS Y COMUNIDADES INDÍGENAS. DERECHO A SER CONSULTADOS. REQUISITOS ESENCIALES PARA SU CUMPLIMIENTO. Tesis: 2a. XXIX/2016 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. II, junio de 2016, p. 1212.

RECURSO DE REVISIÓN PREVISTO EN EL ARTÍCULO 49 DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL. ES IMPROCEDENTE CONTRA LAS RESOLUCIONES EMITIDAS POR LA UNIDAD DE ENLACE DE LA COMISIÓN FEDERAL DE TELECOMUNICACIONES EN LAS QUE COMUNICA SOBRE LA CLASIFICACIÓN DE INFORMACIÓN. Tesis: 2a./J. 137/2015 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. II, octubre de 2015, p. 1976.

SINDICATOS, FEDERACIONES Y CONFEDERACIONES. EL ARTÍCULO 358, FRACCIÓN IV, DE LA LEY FEDERAL DEL TRABAJO, AL ESTABLECER EL DEBER DE SU DIRECTIVA DE RENDIR CUENTA COMPLETA Y DETALLADA DE LA ADMINISTRACIÓN DE SU PATRIMONIO, NO VIOLA EL DERECHO DE ACCESO A LA INFORMACIÓN Y DE PROTECCIÓN DE DATOS PERSONALES (LEGISLACIÓN VIGENTE A PARTIR DEL 1 DE MAYO DE 2019). Tesis: 2a./J. 10/2021 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. II, marzo de 2021, p. 1651.

SISTEMAS DE PROTECCIÓN DE DATOS PERSONALES Y DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. PRECEPTOS CONSTITUCIONALES QUE LOS REGULAN. Tesis: I.2o.A.E.1 CS (10a.), Décima Época, Gaceta del Semanario Judicial de la Federación, t. III, febrero de 2017, p. 2364.

TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. EL ARTÍCULO 12 DE LA LEY RELATIVA DEL ESTADO DE JALISCO, AL CONTEMPLAR COMO "SUJETOS OBLIGADOS" A ORGANISMOS CIUDADANOS, INSTITUCIONES PRIVADAS Y ORGANISMOS NO GUBERNAMENTALES QUE RECIBAN, ADMINISTREN O APLIQUEN RECURSOS PÚBLICOS, CONTRAVIENE EL ARTÍCULO 6o. DE LA CONSTITUCIÓN FEDERAL. Tesis: III.2o.T.Aux.2 A, Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XXXI, marzo de 2010, p. 3086.

TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA EN EL ESTADO DE JALISCO. LA LEY RELATIVA Y EL REGLAMENTO DEL MUNICIPIO DE GUADALAJARA NO TRANSGREDEN EL DERECHO DE AUDIENCIA PREVIA PREVISTO EN EL ARTÍCULO 14 CONSTITUCIONAL. Tesis: PC.III.A. J/6 A (11a.) Semanario Judicial de la Federación, Undécima Época, t. II, diciembre de 2021, p. 2124.

TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL. PRINCIPIOS FUNDAMENTALES QUE RIGEN ESE DERECHO. Tesis: I.8o.A.131 A, Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XXVI, octubre de 2007, p. 3345.

Legislación y normatividad

Acuerdo mediante el cual se aprueban los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales.

Acuerdo mediante el cual se aprueban los criterios de interpretación emitidos por Instituto Nacional de Transparencia, acceso a la Información y Protección de datos personales, en términos de los artículos 199 y 200 de la Ley General de Transparencia y Acceso a la Información Pública y 172 y 173 de la Ley Federal de Transparencia y Acceso a la Información Pública

Criterios para la formulación de Cláusulas en Contratos que tengan por objeto el tratamiento de Datos Personales.

Convenio número 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.

Declaración Universal de los Derechos Humanos.

Decreto por el que se aprueba el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y su Protocolo Adicional relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos, hechos en a Estrasburgo, Francia, el 28 de enero de 1981, y el 8 de noviembre de 2001, respectivamente.

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 n° L 281 de 23/11/1995.

Directiva 2003/98/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público.

DIRECTIVA 2007/2/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 14 de marzo de 2007 por la que se establece una infraestructura de información espacial en la Comunidad Europea (Inspire).

DIRECTIVA (UE) 2019/1024 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 20 de junio de 2019 relativa a los datos abiertos y la reutilización de la información del sector público.

Estándar de Metadatos para la Interoperabilidad Jurídica de Repositorios Universitarios.

Ley Federal de Telecomunicaciones y Radiodifusión.

Ley Federal de Transparencia y Acceso a la Información Pública.

Ley Federal de Protección de Datos Personales en Posesión de Particulares.

Ley de Transparencia y Acceso a la Información Pública Gubernamental. (abrog)

Ley del Sistema Nacional de Información Estadística y Geográfica.

Ley General de Archivos.

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

Ley General de Transparencia y Acceso a la Información Pública.

Norma Técnica para la elaboración de Metadatos Geográficos.

Norma Técnica para la Elaboración de Metadatos para proyectos de generación de Información Estadística Básica y de los componentes estadísticos derivados de proyectos geográficos.

Pacto Internacional de Derechos Civiles y Políticos.

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

Reglamento (CE) No 45/2001 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, [en línea] Diario Oficial de las Comunidades Europeas, 12 de enero de 2001.

Reglamento (CE) 1205/2008 de la Comisión, de 3 de diciembre de 2008, por el que se ejecuta la Directiva 2007/2/CE del Parlamento Europeo y del Consejo en lo que se refiere a los Metadatos.

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, Diario oficial de la Unión Europea de 04 de mayo de 2016.

Tratado de Ámsterdam por el que se modifican el Tratado de la Unión Europea, los Tratados Constitutivos de las comunidades europeas y determinados actos conexos, [en línea] Diario Oficial de las Comunidades Europeas, 10 de noviembre de 1997.