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

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS

“DISEÑO DE UN SISTEMA DE GESTIÓN DE DATOS PERSONALES PARA EL ALUMNADO, CUERPO DOCENTE Y PERSONAL ADMINISTRATIVO DE LA UNIVERSIDAD POLITÉCNICA DE TEXCOCO”

PROPUESTA DE INTERVENCIÓN
Que para obtener el grado de MAESTRO EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Presenta:

Omar Alberto Balcázar Sánchez

Asesora:

Mtra. Evelyn Téllez Carvajal

Ciudad de México, junio de 2020.

Autorización de Impresión

INFOTEC
POSGRADOS

AUTORIZACIÓN DE IMPRESIÓN Y NO ADEUDO EN BIBLIOTECA

MAESTRÍA EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Ciudad de México, 28 de octubre de 2020
INFOTEC-DAIC-GCH-SE-0576/2020.

La Gerencia de Capital Humano / Gerencia de Investigación hacen constar que el trabajo de titulación intitulado

DISEÑO DE UN SISTEMA DE GESTIÓN DE DATOS PERSONALES PARA EL ALUMNADO, CUERPO DOCENTE Y PERSONAL ADMINISTRATIVO DE LA UNIVERSIDAD POLITÉCNICA DE TEXCOCO

Desarrollado por el alumno **Omar Alberto Balcázar Sánchez** y bajo la asesoría de la **Mtra. Evelyn Téllez Carvajal**; cumple con el formato de biblioteca. Por lo cual, se expide la presente autorización para impresión del proyecto terminal al que se ha hecho mención.

Asimismo se hace constar que no debe material de la biblioteca de INFOTEC.

Vo. Bo.

Mtra. Julieta Alcibar Hermosillo
Coordinadora de Biblioteca

Anexar a la presente autorización al inicio de la versión impresa del trabajo referido que ampara la misma.

C.p.p Servicios Escolares

Agradecimientos

A mi familia.

Por su inagotable apoyo e impulso:

A mi padre y madre Alberto y Benita, y a mis hermanos Gerardo y Eloy.

Al cuerpo directivo de la Universidad Politécnica de Texcoco.

Por la oportunidad de permitirme enfocar el presente trabajo en esta institución:

Al rector Mtro. Alberto Sánchez Flores.
Al director académico Mtro. Héctor Manuel Gómez Martínez.
A la profesora Ing. María Guadalupe Leyva Soto.

Al INFOTEC:

A todo el claustro de docentes del cuál recibí certera y oportuna instrucción a lo largo de todo este proceso, en especial a la Mtra. Evelyn Téllez Carvajal por su siempre paciente y acertado apoyo en el desarrollo del presente.

A mis amigos:

A mis amigos y amigas Ariadna, Adriana, Francisco y Edgar por estar siempre ahí, cuando más se les necesita.

Tabla de contenido

Índice de figuras

Índice de cuadros

Siglas y abreviaturas

CIDH	Corte Interamericana de Derechos Humanos
CURP	Clave Única de Registro de Población
INFOTEC	Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación
IdC	Internet de las Cosas
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
Infoem	Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México
Ley general	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
Ley local de protección de datos.	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios
MGO	Manual de Organización de la Univesidad Politécnica de Texcoco
OEA	Organización de Estados Americanos
ONG	Organizaciones no Gubernamentales
PEMPDP	Programa Estatal y Municipal de Protección de Datos Personales
RIPD	Red Iberoamericana de Protección de Datos
SCJN	Suprema Corte de Justicia de la Nación
SGPD	Sistema de Gestión de Protección de Datos
SI	Sociedad de la Información
TIC	Tecnologías de la Información y Comunicación
UE	Unión Europea
UPTex	Universidad Politécnica de Texcoco

Introducción

La presente propuesta de intervención tiene como objetivo principal dotar a la comunidad de la Universidad Politécnica de Texcoco de una herramienta de gestión de datos personales a fin de que alumnos, cuerpo docente y personal administrativo de la institución puedan estar seguros de que sus datos personales están siendo tratados de conformidad con lo establecido por las leyes de la materia y en estricto cumplimiento con los derechos y obligaciones contemplados en dichos ordenamientos, ya que como se explicará más adelante, la Universidad en comento es considerada un sujeto obligado respecto al cumplimiento de la Ley de Protección de Datos correspondiente del estado de México.

Es una realidad que en nuestro país aún hoy en día existan áreas de oportunidad en el tema del tratamiento de datos personales, tal es el caso del estudio que se presenta, pues derivado de la oportunidad de haber cursado la Maestría en Derecho de las Tecnologías de la Información y Comunicación en el INFOTEC, es que se obtuvieron elementos que permitieron el desarrollo de esta investigación aplicada que conjuga tanto los elementos jurídicos de la protección de datos como los beneficios que otorgan los avances científicos que en esta ocasión se presentan en forma de un sistema de gestión de datos personales que permita el cumplimiento de deberes y obligaciones de un sujeto obligado en beneficio de la protección de los datos personales de todos y cada uno de los miembros de la comunidad universitaria para el cual es diseñado.

Siendo así, en el primer capítulo de este trabajo, se expone el marco conceptual del trabajo a partir de las categorías básicas con definiciones de los conceptos que se utilizaron a lo largo de la investigación.

De esta manera, por medio del análisis documental, en el primer capítulo se estudian los conceptos básicos para comprender la protección de la información, los datos personales, la privacidad y la figura de la universidad pública en relación a sus obligaciones con la protección de datos personales que se administran y gestionan en una institución de este tipo como base del resto de la investigación.

Con todo ello, el ofrecer la definición de los conceptos elementales en el presente capítulo, permitirá que el lector pueda contextualizar más claramente la materia de la protección de datos personales y los temas que por añadidura se relacionan a la materia. También se considera importante ofrecer la definición que sobre privacidad se tiene que, aunque siendo una terminología difícil de unificar y concentrar, se dan los aspectos elementales que sobre ella han desarrollado los expertos en la materia.

Una vez esgrimidos los conceptos abordados en el capítulo que antecede, se da paso al capítulo dos en donde se ofrece una descripción general de la institución educativa sobre la cual se diseñará el SGDP, siendo esta la UPTex. Además, se abordará la naturaleza jurídica de referida institución para poder con ello contextualizar la obligación jurídica que tiene al ser un sujeto obligado a la protección de datos personales de las personas que son parte de algún proceso interno afín a la esencia y objetivo de institución que es la impartición de educación universitaria.

También, en el capítulo segundo se presenta el marco jurídico aplicable a la protección de datos personales en México, con la intención de brindar al lector el contexto normativo observable en dicha materia por los sujetos obligados catalogados con acuerdo a la Ley local de protección de datos, resaltándose específicamente la obligación que tienen este tipo de instituciones sobre tener en funcionamiento un SGDP como el que en este trabajo se propone en diseño.

No es óbice mencionar a lo anterior que se han encontrado algunas áreas grises del derecho nacional en la materia, por lo que resulta necesario recurrir a estándares internacionales que son reconocidos por el Estado Mexicano para lograr cubrir todas y cada una de las obligaciones que el sujeto obligado tiene ante el tema de la protección de datos personales.

Así, finalmente en el tercer capítulo, se propone el diseño del SGDP para la UPTex como propuesta para que este sujeto obligado observe cabalmente la normatividad en la materia y con ello la misma institución universitaria pueda dar cumplimiento a las obligaciones que tiene en la materia y se cristalice en beneficio

para todas las personas de la comunidad de esta institución universitaria. Es importante recalcar que las herramientas tecnológicas que se sugieren en esta primera etapa del sistema de gestión son incipientes, por lo que se dejan sentadas las bases para que, de aprobarse por las autoridades correspondientes, esta propuesta pueda ser continuada con el estudio más a fondo de las herramientas tecnológicas que la institución requiere para poder llevar a cabo un correcto funcionamiento del sistema aquí planteado.

Finalmente, es preciso señalar que en el presente trabajo no se ha llevado a profundidad y detalle el tema de las soluciones tecnológicas y costo de su implementación pues aún se requiere la aprobación de las autoridades de este proyecto para poder continuar con el siguiente paso que es el referente a la elaboración e implementación del SGDP que aquí se propone en su diseño.

Capítulo 1

Conceptos fundamentales sobre los datos personales, la privacidad y las universidades públicas como sujetos obligados a la protección de la información personal

Capítulo 1. Conceptos fundamentales sobre los datos personales, la privacidad y las universidades públicas como sujetos obligados a la protección de la información personal

Los avances y desarrollos tecnológicos surgidos en las últimas décadas del siglo pasado —y más notoriamente en las décadas que van del siglo actual—, han tenido un impacto profundo y marcado en amplios sectores de la actual sociedad. Aspectos económicos, estructuras del derecho, relaciones sociales e interpersonales, concepción del tiempo e interpretación de los espacios, son algunos de los ejemplos en donde se puede percibir el impacto a partir de la expresión y manifiesto de la técnica y su discurso.

Centrado en este contexto, y originado a partir del cada día mayor uso de las ya denominadas “tecnologías de la información y comunicación”, o “nuevas tecnologías”, gran parte de las organizaciones tanto de índole privada como pública, basan y dependen de sus procesos internos en la disponibilidad, integridad y confiabilidad de la información que ostentan. Esto, además de traer consigo importantes oportunidades y áreas de explotación económicas, da espacio para que paralela e inevitablemente se creen cuadros de riesgo tanto para las personas naturales como para las organizaciones que de alguna u otra manera depositan y confían su información en dispositivos y procesos electrónicos y digitales expuestos a peligros inherentes a tal naturaleza.

La protección de la información en forma de datos personales en las organizaciones tanto de índole privada como pública se ha convertido ya en un imperativo jurídico-organizacional que tendría que ser observado por estas entidades para con ello poder cumplir con lo establecido en la normatividad mexicana aplicable a la materia. Así pues, en este capítulo se ofrece la descripción de los conceptos elementales relativos a la protección de datos personales, mismos que permitirán tener una idea clara sobre el tema fundamental del presente trabajo en su conjunto. Se parte del concepto fundamental de dato personal hasta el significado de la universidad pública y la relación existente entre

ambos conceptos, esto debido a que el proyecto que se llevó a cabo tiene como objetivo principal la protección de datos personales que se administran y gestionan en una institución de este tipo.

Para poder presentar al lector el marco conceptual del trabajo, se realizó una selección de categorías básicas a definir, se procedió a la elaboraron de ficheros con definiciones de los conceptos que se utilizan en el presente capítulo para con ello ofrecer el marco teórico sustancial de la investigación en su conjunto.

El ofrecer la definición de los conceptos elementales en el presente capítulo, permitirá que el lector pueda contextualizar más claramente la materia de la protección de datos personales y los temas que por añadidura se relacionan a la materia. Una de las categorías seleccionadas sin duda es la “privacidad” que, aunque es una terminología difícil de unificar y centrar, se dan los aspectos elementales que sobre ella expertos en la materia han desarrollado. Esto es importante dado que la protección de los datos personales es considerada por algunos autores como parte del derecho a la privacidad, como derecho humano plasmado en diferentes instrumentos jurídicos de carácter internacional a los que el Estado mexicano se encuentra obligado a cumplir y observar.

Una vez entendidos los conceptos abordados en este capítulo, se da paso al capítulo siguiente en donde se ofrece una descripción general de la institución educativa sobre la cual se diseñará el sistema de gestión de datos personales, siendo esta la Universidad Politécnica de Texcoco. También se abordará la naturaleza jurídica de la mencionada institución para poder con ello contextualizar la obligación jurídica que tiene al ser un sujeto obligado a la protección de los datos personales de todas las personas que forman parte de algún proceso interno afín a la esencia y objetivo de institución que es la impartición de educación universitaria.

1.1 Los datos personales y el derecho a su protección

Para dar inicio al primer subtema, es preciso y necesario hacer la observación de que en posteriores apartados de este trabajo se hará referencia a la privacidad y al

derecho a su protección, con la finalidad de que el lector pueda percibir de que el derecho a la protección de los datos personales es un concepto concebido por diferentes tratadistas y especialistas en la materia como un derecho autónomo y desligado del derecho a la protección de la privacidad, siendo, por tanto, derechos concebidos, estudiados y protegidos de forma distinta en México.

Como se mostrará más adelante, esta diferenciación planteada por tales especialistas resulta ser tan trascendental, que incluso tal derecho ha sido elevado a rango constitucional en varios países instituyéndose de tal forma, como derecho a la protección de datos personales.

En ese sentido, a continuación, se ofrecen algunos ejemplos de constituciones de países con disposición constitucional expresa en relación con la protección de datos personales.

Cuadro 1. Países con reconocimiento constitucional al derecho a la protección de datos personales.

PAÍS	ARTÍCULO CONSTITUCIONAL	CONTENIDO
Argentina	Artículo 43	Toda persona podrá interponer esta acción para tomar conocimiento de los *datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos.* No podrá afectarse el secreto de las fuentes de información periodística.
Ecuador	Artículo 66.19	El derecho a la protección de *datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección*. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.
Paraguay	Artículo 135	Toda persona puede acceder a la información y a los *datos que sobre si misma*, *o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad*. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos.
Portugal	Artículo 35	1. Derechos de los ciudadanos. 2. La ley define el concepto de *datos personales*, y las condiciones aplicables a su tratamiento automatizado, conexión, transmisión y utilización, y garantiza su protección por medio de un órgano administrativo independiente. 3. Límites utilización de la

		informática. 4. Prohibición Acceso a los datos personales de terceros, salvo en casos excepcionales previstos por la ley. 5. Prohibida la atribución de un número nacional único a los ciudadanos. 6. Acceso libre general garantizado a las redes informáticas para uso público, definiendo la ley el régimen aplicable a los flujos transfronterizos de datos y las formas apropiadas de protección de datos personales. 7. *Protección datos personales mantenidos en ficheros manuales.*
República Dominicana	Artículo 44.2	Toda persona tiene el derecho a acceder a la información y a los *datos que sobre ella o sus bienes reposen en los registros oficiales o privados*, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por la ley. El tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad. Podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos.
Venezuela	Artículo 28	*Toda persona tiene derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados* (…) conocer el uso que se haga de los mismos y su finalidad, y a solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas (…).

Fuente: Elaboración propia, con información adaptada tomada de Daniel A. López Carballo "Protección de datos y *habeas data:* una visión desde Iberoamérica".[1]

En México, nuestra carta magna lo instituye de la siguiente forma en el artículo 16, segundo párrafo:

> 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

[1] López Carballo, Daniel A. (coord.), "Protección de datos y habeas data: una visión desde Iberoamérica" [en línea], con motivo de la XVIII Edición del Premio Protección de Datos Personales de Investigación, España, Agencia Española de Protección de Datos, 2015, p. 202, disponible en: *http://bgbg.mx/wordpress/wp-content/uploads/2015/06/Proteccion_de_datos_y_habeas_data.pdf*, última fecha de consulta el 31 de octubre de 2019.

de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Del análisis del contenido de la tabla previamente ofrecida, resaltan los siguientes planteamientos:

1.- Las disposiciones constitucionales de los países de Paraguay, República Dominicana y Venezuela hacen el señalamiento expreso de que en caso de que cualquier persona decidiera solicitar o ejercitar algún derecho en relación al tratamiento de sus datos personales, lo manifestasen a través de un mecanismo o vía “jurisdiccional”, por medio de un “magistrado competente”, “autoridad judicial” o “tribunal competente”, situación distinta a lo establecido en México, en donde tal situación tendría que ser dirimida por un organismo autnónomo, en este caso, el INAI.

2.- Otro punto que llama la atención, es lo establecido en la constitución portuguesa en relación a los “flujos transfronterizos de datos”, ya que como puede apreciarse en las demás constituciones, en ninguna de estas se encuentra tal manifestación, situación similar a lo estipulado en la constitución mexicana. Quizá sea la justificación de tal referencia el hecho de que Portugal pertenece a la Unión Europea y por lo tanto se tengan que instituir postulados constitucionales acorde a las demandas y necesidades comerciales en esa región.

Con esto podemos ver la importancia que se le ha dado a la protección de los datos personales a escala mundial, la protección de datos como parte integral de la protección de los derechos humanos junto con la protección a la privacidad que, como ya se ha vertido previamente, se consideran ya dos derechos independientes y autónomos, tanto así, que en diversas constituciones de diferentes naciones se han instituido de tal forma.

Una vez discernido la temática en relación con la autonomía de la protección de los datos personales, a continuación, se exponen las posiciones con relación al concepto dato en un primer lugar, para continuar con concepciones sobre datos personales y finalizar con lo que por datos personales sensibles se concibe.

1.1.1 Concepto de dato

De acuerdo con la Real Academia Española, dato proviene del latín *datum,* "lo que se da".[2] El término dato por sí solo resulta ser un término relativamente ambiguo. En la primera acepción que da la misma Academia se constata esto al establecer: "Información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho".[3] En la segunda acepción que se ofrece a partir de la misma referencia, se hace mención al campo de la informática (*Inform.*) al establecerse como dato: "*Inform*. Información dispuesta de manera adecuada para su tratamiento por una computadora".[4]

En relación a esta última acepción, se puede señalar que no son cualquier tipo de datos los que ocupan al derecho a la protección de datos personales, puesto que como su propia denominación lo da a inferir, el campo de acción de este derecho es la información que identifica o hace identificable a las personas, convirtiéndose consecuentemente en dato personal y no así cualquier otro tipo de datos que se pueden tener registrados y disponibles ya sea en forma física o en cualquier tipo de ordenador y que puede ser utilizado para cualquier proceso administrativo-organizacional.

Resulta importante haber hecho el comentario precedente, puesto que como lo refiere la Dra. Isabel Fernández, "El dato, en sí mismo, no necesita protección alguna. Sin embargo, cuando el dato se une a una persona, es algo distinto. Ya no protegemos, entonces, al dato, sino al titular del mismo, es decir a la persona. Es más, cuando el dato se une a la persona se convierte en información personal".[5]

---

[2] Real Academia Española: diccionario de la lengua española, disponible en: *https://dle.rae.es/?id=Bskzsq5|BsnXzV1*, última fecha de consulta el 31 de octubre de 2019.

[3] *Idem*

[4] *Idem*

[5] Fernández de Marcos, Isabel Davara, "Protección de datos de carácter personal en México: problemática jurídica y estatus normativo actual", en Compendio de

De esta manera, con base en los previos planteamientos, el concepto dato por sí solo, dada la ambigüedad planteada en el párrafo que antecede, y su falta de ligadura a un campo semántico en específico, no representa mayor significado. Sin embargo, existiendo relación con la temática de la protección de datos personales, este retoma mayor consideración cuando se relaciona a una persona, como lo ha referido la Dra. Isabel Fernández, pues son los datos personales la esencia núcleo de protección en el ejercicio del denominado derecho a la protección de datos personales.

1.1.2 Concepto de dato personal

Desde una perspectiva nacional, para el INAI (antes IFAI)[6], los datos personales son "Cualquier información que refiera a una *persona física* que pueda ser identificada a través de los mismos, los cuales se pueden expresar en forma numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, como, por ejemplo: nombre, apellidos, CURP, estado civil, lugar y fecha de nacimiento, domicilio, número telefónico, correo electrónico, grado de estudios, sueldo, entre otros".[7]

Por otra parte, y siguiendo una postura institucional, la actual y vigente ley general establece en su artículo 3 numeral IX, que se entenderá por 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".

---

lecturas y legislación. Protección de datos personales, México, Tiro Corto Editores, 2010, p. 78.

[6] Hasta mayo de 2015 tras la aprobación de la Ley General de Transparencia y Acceso a la Información.

[7] Instituto Federal de Acceso a la Información Pública, "Guía práctica para ejercer el derecho a la protección de datos personales", México, 2015, p. 3. [Las cursivas son propias]

Por otra parte, desde una perspectiva emitida por expertos tratadistas en la materia que conforman la RIPD[8], se define a los datos personales de la siguiente manera: “Cualquier información concerniente a una *persona física* identificada o identificable, expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente, siempre y cuando esto no requiera plazos o actividades desproporcionadas”.

Desde una perspectiva europea, en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo 2016, se establece que se entenderá por datos personales*:*

> …toda información sobre una *persona física* identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la

[8] La RIPD se configura como un foro integrador de los diversos actores, tanto del sector público como privado, que desarrollen iniciativas y proyectos relacionados con la protección de datos personales en Iberoamérica, con la finalidad de fomentar, mantener y fortalecer un estrecho y permanente intercambio de información, experiencias y conocimientos entre ellos, así como promover los desarrollos normativos necesarios para garantizar una regulación avanzada del derecho a la protección de datos personales en un contexto democrático, tomando en consideración la necesidad del continuo flujo de datos entre países que tienen diversos lazos en común y una preocupación por este derecho. Información visible en su página oficial, disponible en: *http://www.redipd.es/la_red/Historia/index-ides-idphp.php* [Las cursivas son propias], última fecha de consulta el 31 de octubre de 2019.

identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.[9]

Finalmente, en el Informe del Comité Jurídico Interamericano de la OEA, se emitieron los Principios Relativos a la Privacidad y Protección de Datos Personales con la finalidad de proporcionar a los Estados parte los elementos básicos para una protección efectiva a la privacidad. Es de hacerse notar que, conforme a lo estipulado en el mismo documento, estos principios se aplican a los sectores público y privado por igual, es decir, tanto a los datos personales generados, recopilados o administrados por entidades públicas como a los datos recopilados y procesados por entidades privadas, y para tal efecto se establece que:

> Tal como se usa en estos principios, la frase "datos personales" abarca la información que identifica o puede usarse de manera razonable para identificar a una persona en particular de forma directa o indirecta, especialmente por referencia a un número de identificación o a uno o más factores referidos específicamente a su identidad física, fisiológica, mental, económica, cultural o social. La frase no abarca la información que no identifica a una persona en particular (o no puede usarse de manera razonable para identificarla).
>
> (…)
>
> A efectos de estos principios, solo la gente (*personas físicas*) tiene intereses en materia de privacidad, a diferencia de los dispositivos, las computadoras o los sistemas mediante los cuales interaccionan.

[9] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), disponible en: *https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679* [Las cursivas son propias], última fecha de consulta el 31 de octubre de 2019.

> Tampoco tienen intereses en materia de privacidad las organizaciones u otras personas jurídicas con las que tratan. Los menores (personas que no han llegado a la edad adulta) también tienen intereses legítimos en materia de privacidad que deben reconocerse y protegerse efectivamente en la legislación nacional.[10]

Como se puede desprender de las cuatro aportaciones sobre el concepto de datos personales, se logra observar un común denominador entre ellas. En las cuatro se hace una delimitación expresa en cuanto a que la información tendrá que referirse o ser concerniente a *personas físicas*, sin que en ninguna de ellas se mencione las *personas jurídico-colectivas*, lo cual puede ser resumido en el siguiente cuadro:

Cuadro 2. Criterios sobre el concepto de datos personales.

Ente emisor	Fecha	Fragmento sobre definición de datos personales
1. INAI	Noviembre de 2015	"Cualquier información que refiera a una **persona física** que pueda ser identificada a través de los mismos…"
2. RIPD.	Junio de 2016	"Cualquier información concerniente a una **persona física** identificada o identificable…"
3. Parlamento Europeo.	Abril de 2016	"…toda información sobre una **persona física** identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente…"
4. OEA.	Marzo de 2015	"A efectos de estos principios, solo la gente (**personas físicas**) tiene intereses en materia de privacidad, a diferencia de los

[10] La finalidad de los Principios de la OEA sobre la privacidad y la protección de datos personales es establecer un marco para salvaguardar los derechos de la persona a la protección de los datos personales y a la autodeterminación en lo que respecta a la información. Los principios se basan en normas reconocidas a nivel internacional. Su intención es proteger a las personas de la recopilación, el uso, la retención y la divulgación ilícitos o innecesarios de datos personales, disponible en: *http://www.redipd.es/documentacion/otrosdocumentos/common/Informe_CJI-doc_474-15_rev2_26_03_15.pdf* [Las cursivas son propias], última fecha de consulta el 31 de octubre de 2019.

		dispositivos, las computadoras o los sistemas mediante los cuales interaccionan".

Fuente: Elaboración propia con base en documentos de organismos especialistas en la materia de protección de datos.

Esta idea en un primer momento consensuada, sobre que los datos personales tienen que pertenecer solamente a personas físicas, parecería no dar espacio a duda o incertidumbre, sin embargo, nuestra SCJN ha emitido un criterio jurisprudencial que aporta otra perspectiva y que pudiera ir en contra de la unificada conceptualización sobre que los datos personales se pueden considerar solamente adjudicables a las personas físicas, y no a las personas jurídico-colectivas, criterio que se reproduce 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.**
>
> 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.[11]

El anterior criterio, sin lugar a duda, motiva a la reflexión y a la deliberación, en el sentido de que se manifiesta algo "novedoso" que no se ha considerado al menos en las conceptualizaciones previamente esgrimidas, esto al señalarse que a las *personas morales* les pueden ser atribuibles, en forma equiparada, datos que se creían solamente ser prerrogativas atribuibles a las personas físicas.

Abona a la reflexión lo que se establece en el artículo 25 del Código Civil Federal al listar las entidades que se consideran *personas morales* con acuerdo a la legislación civil y poder de esta manera tener más elementos de juicio en cuanto al criterio emitido por la SCJN:

> Artículo 25.- Son personas morales:
> I. La Nación, los Estados y los Municipios;
> II. Las demás corporaciones de carácter público reconocidas por la ley;
> III. Las sociedades civiles o mercantiles;
> IV. Los sindicatos, las asociaciones profesionales y las demás a que se refiere la fracción XVI del artículo 123 de la Constitución Federal;
> V. Las sociedades cooperativas y mutualistas;

[11] Tesis: P. II/2014 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, pleno, libro 3, febrero de 2014, tomo I, p. 274. [Las cursivas son propias].

VI. Las asociaciones distintas de las enumeradas que se propongan fines políticos, científicos, artísticos, de recreo o cualquiera otro fin lícito, siempre que no fueren desconocidas por la ley.

VII. Las personas morales extranjeras de naturaleza privada, en los términos del artículo 2736.

Finalmente, de las mismas definiciones de datos personales aportados previamente, podemos concluir lo siguiente:

1. Tanto el concepto formulado por el entonces IFAI, como por el emitido por la RIPD, especifican que las formas en que la información relacionada a las personas puede ser expresada numérica, alfabética, gráfica, etcétera.
2. Por otra parte, tanto lo establecido en el Reglamento General Europeo, como los principios expuestos por la OEA se asemejan al establecer, a diferencia de las dos concepciones previas, que como forma de expresión de la información concerniente a las personas físicas, tendrán que estar *referenciado* a un número de identificación o a uno o más factores referidos específicamente a su identidad física, fisiológica, mental, económica, cultural o social, etcétera.
3. Los dos últimos conceptos, tanto de la Unión Europea, como de la OEA, incorporan características distintas en cuanto a la forma de expresión de la información personal, como por ejemplo *datos de localización*, lo cual demuestra que la formulación de los conceptos previos ha cambiado y que quizá ese cambio sea derivado de las nuevas realidades que el permanente avance de la tecnología genera.
4. Finalmente, sea cual fueren las razones y motivos para proponer nuevas concepciones con relación a los datos personales, pudiera considerarse loable que la misma terminología sea adaptable a los cuerpos normativos aplicables a la materia que a nivel internacional, nacional y local se han promulgado.

Ahora bien, en cuanto el criterio jurisprudencial emitido por la SCJN previamente señalado, se considera que tal discernimiento se desapega

claramente de la esencia núcleo de la protección de datos personales, pues si bien es cierto que las denominadas personas morales se entienden y contemplan como tal dentro de lo instituido en el derecho civil, no dejan de ser un ficticio jurídico ideado, concebido y materializado a partir de la voluntad y control de personas físicas, particularidades mismas que no se encuentran en las personas morales puesto que ellas mismas no se encuentran en potestad y voluntad de ejercer sobre ellas mismas los denominados “autocontrol” y “autodeterminación”, situaciones que sí pueden llevarse a cabo por cualquier persona física estando en pleno uso y goce de sus facultades mentales y jurídicas.

1.1.3 Concepto de dato personal sensible

Por último, a continuación, se ofrece el concepto de dato personal sensible como un campo más específico de información que ostentan las personas físicas, información que, por su propia y especial naturaleza, puede resultar de mayor trascendencia en la protección de las personas al hacerse un mal uso o un uso indebido de esta información.

En ese sentido, es la RIPD la que nuevamente ofrece su concepto al respecto, al considerar a los datos personales sensibles:

> Aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física.[12]

[12] Estándares de Protección de datos personales, RIPD, 2017, disponible en: *http://www.redipd.es/la_red/Historia/index-ides-idphp.php*, última fecha de consulta el 31 de octubre de 2019.

Por su parte, con el mismo propósito de definir a los datos personales sensibles, la OEA establece que:

> La frase *datos personales sensibles* se refiere a una categoría más estrecha que abarca los datos que afectan a los aspectos más íntimos de las personas físicas. Según el contexto cultural, social o político, esta categoría podría abarcar, por ejemplo, datos relacionados con la salud personal, las preferencias sexuales, las creencias religiosas o el origen racial o étnico. En ciertas circunstancias podría considerarse que estos datos merecen protección especial porque, si se manejan o divulgan de manera indebida, podrían conducir a graves perjuicios para la persona o a discriminación ilegítima o arbitraria.
>
> En los principios se reconoce que la sensibilidad de los datos personales puede variar según la cultura y cambiar con el tiempo y que los riesgos de ocasionar daños reales a una persona como consecuencia de la divulgación de datos podrían ser insignificantes en una situación en particular, pero podrían poner en peligro la vida en otra.[13]

Por otra parte, la postura oficial emitida por el congreso general mexicano, establecido en la ley general de la materia, en su artículo 3, fijó la definición de datos personales sensibles de la siguiente forma:

> Artículo 3. Para los efectos de la presente Ley se entenderá por:
>
> (I…IX)
>
> "X. Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera

[13] Principios de la OEA sobre la privacidad y la protección de datos personales, Organización de los Estados Americanos, disponible en: *http://www.redipd.es/documentacion/otrosdocumentos/common/Informe_CJI-doc_474-15_rev2_26_03_15.pdf*, última fecha de consulta el 31 de octubre de 2019.

> 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"

Finalmente, a esta especialización de los datos personales bien cabe la siguiente pregunta y su respuesta al mismo tiempo "¿por qué es trascendente conceptualizar y diferenciar el concepto de dato personal sensible? Porque, no todos los datos personales tienen la categoría de sensibles. Serán considerados datos personales si revelan aspectos de nuestra vida privada, pero serán considerados datos sensibles si son datos que revelan aspectos íntimos de las personas".[14]

Al igual que el concepto de dato personal, el concepto de dato personal sensible, aplicado al mundo jurídico, representa una convención que muy probablemente sufrirá alguna variación en su concepción al tener que adaptarse a los nuevos y diferentes contextos que la tecnología habrá de imprimir en todos los aspectos de la vida social con el trascurso del tiempo.

La concepción de privacidad, al igual que muchos otros conceptos, tendrá que adaptarse a los aún desconocidos contextos que la tecnología -cada vez más invasiva, por cierto- impondrán y ejercerán en el futuro, teniendo como consecuencia que lo ahora concebido como dato personal sensible, quizá implique otros aspectos del cuerpo y de la psique humana que por ahora no se logran concebir, configurándose de esta forma lo dicho de que en derecho es peligroso establecer definiciones.

---

[14] Cristea Uivaru, Lucia Nicole, "La protección de datos de carácter sensible en el ámbito europeo. Historia clínica digital y big data en salud" [en línea], tesis doctoral, Universitat Abat Oliba CEU, 2017, disponible en: *https://www.tdx.cat/bitstream/handle/10803/442972/Tlcu.pdf?sequence=1&isAllowed=y*, última fecha de consulta el 31 de octubre de 2019.

1.2 La privacidad de la información personal en el siglo XXI

La creciente preocupación por la protección a la privacidad de las personas en muchos sectores de la sociedad, derivada de una cada vez mayor dependencia de los procesos automatizados desarrollados en las denominadas TIC, es un hecho al parecer en constante crecimiento.

Esta inquietud ha sido percibida en forma colectiva tanto por gobiernos nacionales como organizaciones representantes de la sociedad civil, el sector privado, instituciones académicas y las Naciones Unidas y sus organismos especializados. Como ejemplo de esto se estableció en la Cumbre Mundial sobre la SI[15] realizada en diciembre de 2003 en Ginebra, Suiza, en la que se adoptaron dos documentos, siendo ellos una Declaración de Principios y un Plan de Acción. En la parte de la Declaración de Principios, en el punto 35 se acordó fomentar:

[15] Sitio oficial de la Cumbre Mundial de la Sociedad de la Información, CMSI-ONU, disponible en: *https://www.itu.int/net4/wsis/forum/2019/es/* [Las cursivas son propias], última fecha de consulta el 18 de julio de 2019. El Foro de la Cumbre Mundial de la Sociedad de la Información (CMSI) es una plataforma mundial de múltiples partes interesadas de las Naciones Unidas (ONU) que facilita la implementación de las Líneas de Acción de la CMSI para avanzar en el logro de los Objetivos de Desarrollo Sostenible (ODS). Está organizado conjuntamente por la UIT, la UNESCO, el PNUD y la UNCTAD, en estrecha colaboración con todos los co-facilitadores de las Líneas de Acción de la CMSI y otros organismos de las Naciones Unidas (DAES, FAO, PNUMA, OMS, ONU Mujeres, OMPI, PMA, OIT, OMM, CCI, UPU, ONUDD, UNITAR, UNICEF y Comisiones regionales de las Naciones Unidas). Representa la mayor reunión mundial de la comunidad de 'las TIC para el desarrollo'. Supone una oportunidad para el intercambio de información, la creación de conocimiento y la compartición de prácticas óptimas, al tiempo que para identificar tendencias emergentes y fomentar las asociaciones, teniendo en cuenta la evolución de las sociedades de la información y el conocimiento,

> …un clima de confianza, incluso en la seguridad de la información y la seguridad de las redes, la autenticación, *la privacidad* y la protección de los consumidores, es requisito previo para que se desarrolle la Sociedad de la Información y para promover la confianza entre los usuarios de las TIC. Se debe fomentar, desarrollar y poner en práctica una cultura global de ciberseguridad, en cooperación con todas las partes interesadas y los organismos internacionales especializados. Se deberían respaldar dichos esfuerzos con una mayor cooperación internacional. Dentro de esta cultura global de ciberseguridad, es importante mejorar la seguridad y garantizar la protección de los datos y *la privacidad*, al mismo tiempo que se amplía el acceso y el comercio. Por otra parte, es necesario tener en cuenta el nivel de desarrollo social y económico de cada país, y respetar los aspectos de la Sociedad de la Información orientados al desarrollo.

En ese mismo sentido y como segundo ejemplo de organismos internacionales preocupados por la protección a la privacidad, encontramos a la Organización No Gubernamental (en adelante ONG) *Privacy International* que, en su página oficial, como parte de su cometido institucional se puede leer lo siguiente:

> Privacidad internacional es una organización beneficiaria que reta a los gobiernos y compañías que quieren saber todo sobre los individuos, grupos y la sociedad en su conjunto. El futuro que Privacidad Internacional quiere es uno en donde la gente esté en control de sus datos y de la tecnología que usan, y que los gobiernos y las compañías no sean capaz más de usar la tecnología para monitorear, rastrear, analizar, perfilar, y al final de todo, manipularnos y controlarnos. Pero tenemos que pelear por ese futuro.[16]

[16] Sitio oficial de Privacidad Internacional, Privacy International, disponible en: *https://privacyinternational.org/es/about*, última fecha de consulta el 18 de julio de 2019. Privacy International is a charity that challenges the governments and

Un ejemplo más de este tipo de organizaciones preocupadas por la protección de la intimidad, lo encontramos ahora en un contexto latinoamericano en donde la ONG denominada "Derechos Digitales"[17] ha establecido como su objetivo fundamental, el desarrollo, la defensa y la promoción de los derechos humanos en el entorno digital, desplegando su actuar en tres ejes fundamentales:

a) Libertad de expresión.
b) Privacidad y datos personales, y;
c) Derechos de autor y acceso al conocimiento.

Podemos encontrar, como se puede leer en las tres proclamas previamente presentadas, conceptos como Sociedad de la Información, Tecnologías de la Información y Comunicación, y entorno digital.

Hasta este momento podemos resumir, a partir de las tres visiones anteriores, que se comparte de alguna u otra manera la inquietud de proteger a la intimidad de las personas en los entornos digitales derivado del uso, aprovechamiento y explotación de las TIC en lo que se ha denominado la SI.[18]

---

companies that want to know everything about individuals, groups, and whole societies. The future PI (Privacy International) wants is one where people are in control of their data and the technology they use, and governments and companies are no longer able to use technology to monitor, track, analyse, profile, and ultimately, manipulate and control us. But we have to fight for that future. [Traducción libre]

[17] Página oficial de la ONG "Derechos Digitales", disponible en: *https://www.derechosdigitales.org/quienes-somos/derechos-digitales/*, última fecha de consulta el 31 de octubre de 2019.

[18] Katz, Jorge, "Los caminos hacia una sociedad de la información en América Latina y el Caribe (CEPAL), página oficial de la CEPAL, disponible para su consulta en: *https://repositorio.cepal.org/bitstream/handle/11362/2354/2/S034237_es.pdf*, última fecha de consulta, el 17 de julio de 2019.

Es precisamente en la llamada SI en donde se hace uso de las TIC a escala masiva y con resultados industriales; es aquí mismo en donde se puede percibir a la información como la materia fundacional y fundamental en el desarrollo de dichos procesos tecnológicos teniendo también como materia prima a la información personal, como una especie de lo que genéricamente se ha conceptualizado como información. Esto se reafirma con la siguiente idea:

> No hay duda que (sic) el uso y el acceso a la información son factores críticos en el desarrollo de la economía actual y son las Tecnologías de la Información y las Comunicaciones (TIC) las que han permitido que el acceso a los grandes volúmenes de información sea relativamente sencillo, eficiente y eficaz, por lo cual se puede afirmar que parte de la

---

Sobre el concepto SI se presenta una divergencia conceptual al respecto que no nos permite encontrar una definición clara, concreta y unívoca. Por ejemplo, en el documento el autor establece que “El concepto de Sociedad de la Información es muy complejo y su nivel de desarrollo es aún incipiente. (...) El marco conceptual que caracteriza este paradigma se basa en las tecnologías de la información y las comunicaciones (TIC) y del proceso de digitalización resultante,

Sin embargo, y con el objetivo de precisar un poco más la importancia de los eventos que se suceden en la denominada SI, se considera preciso señalar lo que la ONU declaró como principio en la Cumbre Mundial de la Sociedad de la Información en el punto 1, que “… los representantes de los pueblos del mundo, (…) con motivo de la primera fase de la Cumbre Mundial sobre la Sociedad de la Información, declaramos nuestro deseo y compromiso comunes de construir una Sociedad de la Información centrada en la persona, integradora y orientada al desarrollo, en que todos puedan crear, consultar, utilizar y compartir la información y el conocimiento…”, documento disponible en: *https://www.itu.int/net4/wsis/forum/2019/es/*, última fecha de consulta el 18 de julio de 2019.

> consolidación de la SI ha sido posible gracias al desarrollo vertiginoso de las TIC.[19]

Este contexto, originado a partir del cada día mayor uso de las TIC, además de traer consigo importantes oportunidades y áreas de explotación económicas, da espacio para que paralela e inevitablemente se creen cuadros de riesgo tanto para las personas naturales como para las organizaciones de todo tipo que de alguna u otra manera depositan y confían la información que ostentan en dispositivos electrónicos y tienen la necesidad de conectarse al internet.

> En efecto, la posibilidad que ofrecen los medios informáticos y las redes de comunicación de archivar, organizar, sistematizar, reproducir y difundir, de manera prácticamente ilimitada, los datos y las informaciones de carácter personal, suponen una incuestionable amenaza para los derechos fundamentales, y muy en especial para los que protegen la privacidad.[20]

Con lo descrito previamente, se hace constancia de que es en la SI en donde el rol de las llamadas TIC ostentan especial y evidente importancia. También podemos señalar que, entre otros elementos, la información es el componente primordial que caracteriza y da funcionamiento a esta sociedad a traves de la masiva obtención, acaparamiento y tratamiento de dicha información.

Claro resulta ser que, como se ha mencionado previamente, una especie de esa información genérica lo es la información personal que puede ser obtenida y

---

[19] Sánchez Torres, Jenny Marcela, *et.al.*, *"*La sociedad de la información: Génesis, iniciativas, concepto y su relación con Las TIC", *Revista UIS Ingenierías*, Colombia, vol. 11, núm. 1, enero-junio, 2012, disponible en: *http://www.redalyc.org/articulo.oa?id=553756873001*, última fecha de consulta el 31 de octubre de 2019.

[20] Díaz Revorio, Francisco Javier, *Los derechos humanos ante los nuevos avances científicos y tecnológicos. Genética e internet ante la Constitución,* México, Tirant lo Blanch-Comisión Nacional de Derechos Humanos, 2009, p. 177.

recabada en la red a través de procesos algorítmicos muy sofisticados y de gran potencia que hacen que la obtención de la información se reduzca a tan sólo básicos comandos a los ordenadores al estar conectados al internet.[21]

Es en este contexto en donde las amenazas a la privacidad de las personas se hacen evidentes al exponer, sin ninguna cautela o precaución, información personal que pudiera ser utilizada en determinado momento por otras personas

[21] No es el objetivo principal del presente trabajo profundizar sobre lo que es llamado internet, sin embargo, muchos tratadistas y expertos en la materia establecen que la importancia del internet en la denominada SI se potencializa dado que a través de esta "red de redes" o "autopista de la información" es por donde "viajan" ingentes cúmulos de información que, con apoyo en potentes ordenadores y determinadas operaciones algorítmicas, productos característicos de las TIC, las grandes corporaciones y los gobiernos de muchos países pueden obtener y acumular dicha información, "En el caso de la navegación por Internet, por ejemplo, las empresas y prestadores de servicios nos ofrecen de forma gratuita sus motores de búsqueda, páginas webs y servicios asociados, para leer la prensa, consultar la previsión meteorológica, o estar en contacto con otras personas a través de redes sociales o foros. No obstante, cada vez que entramos en una web estamos descargando automáticamente una serie de microprogramas conocidos como cookies que recaban información de nuestra actividad online y hacen llegar al propietario de la web visitada información sobre nuestra IP, MAC o IMEI (la matrícula de nuestro dispositivo), el tiempo y forma en que utilizamos un sitio concreto u otros sitios que estén abiertos en el mismo momento, identifica si somos visitantes habituales y qué uso hacemos de la página de internet, en qué secuencia y cómo accedemos a otros sitios, etcétera". Galdón Clavell, Gemma, "¿Qué hacen con nuestros datos en intenet?", *El país* [en línea], junio 2015, disponible en: *https://elpais.com/tecnologia/2015/06/12/actualidad/1434103095_932305.html*, última fecha de consulta 18 de julio de 2019.

con intenciones no solamente contemplativas o de admiración, sino con fines y propósitos ilícitos que pudiera poner en peligro la integridad de los individuos.

> Pero ahora interesa destacar que la protección de la vida privada frente a Internet implica el reconocimiento de nuevas dimensiones de la misma, habitualmente no incluidas en la preservación de la intimidad. Se trataría, por así decirlo, de un derecho a la "privacidad informática" o "privacidad virtual", aunque acaso hablaríamos más propiamente de una nueva dimensión de los derechos reconocidos en el artículo 18 de la Constitución o el artículo 8 del Convenio de Roma".[22]

Sin soslayar lo anterior, es importante recalcar que el objetivo principal del presente trabajo está dirigido a aquella información personal que ostenta una institución educativa pública que de acuerdo con la legislación nacional y local aplicables a la materia, debe de ofrecer un tratamiento a los datos personales conforme la normatividad lo establece y ofrecer de esa manera los mayores rangos de protección a la información que han recabado y tienen, además, la obligación de proteger consecuentemente la privacidad de todos los actores que intervienen en sus procesos diarios afines a su objetivo central que es la impartición de educación con carácter de pública.

Hasta este momento, se ha hecho alusión a la importancia de la información en la SI y los riesgos implícitos a la privacidad a partir de un inadecuado o malintencionado uso de la información personal que se lleva a cabo en el entorno de las TIC y en especial en el mundo del internet, pero, a todo esto, ¿qué debemos entender por privacidad?

1.2.1 Concepto de privacidad

Antes de dar comienzo al siguiente apartado, se considera oportuno hacer la aclaración de que, si bien es cierto que en el presente trabajo se hace sustancial referencia tanto al derecho a la protección de datos personales como al derecho a la privacidad, en ningún momento tendrán que considerarse ambos derechos

[22] Díaz Revorio, Francisco Javier, *op. cit.*, nota 21, p. 193.

como el mismo, puesto que como ya previamente se ha señalado, la complejidad y especialización que ha tenido lugar en el campo de la protección de los datos personales, hace que éste último sea ya considerado por muchos tratadistas en la materia como un derecho autónomo e independiente.

En ese sentido, el derecho a la protección de datos personales se entiende como aquel que tiene una persona a saber quién, cómo y para qué se tratan sus datos personales, mientras que por derecho a la privacidad se entiende en el sentido de proteger a la persona de injerencias o intromisiones indebidas en su privacidad, coincidiendo así en lo esencial con el derecho a la protección de datos personales, o incluso, si se quiere, considerar al segundo como especie del primero, pero sin considerarse como el mismo.

Así pues, el poder dar el concepto de privacidad representado ya en sí, una relevante complicación metodológica. Esto derivado a partir de que, al momento de hacer la búsqueda de referencias bibliográficas al respecto, se pudo advertir, por un lado, que existen autores con una marcada divergencia y falta de unificación en torno a la conceptualización.

Por otra parte, se pudo percibir la existencia de otros autores que ofrecen un concepto un poco más concreto y definido que, para los propósitos del presente trabajo, serán los que deberán de ser considerados.

Para iniciar, el profesor Daniel Solove, de la Universidad de Derecho George Washington, lo manifiesta de la siguiente manera:

> La privacidad, sin embargo, es un concepto en desorden. Nadie puede articular lo que significa. Actualmente, la privacidad es un concepto en barrida, abarcando (entre otras cosas) libertad de pensamiento, control sobre el cuerpo de uno, soledad en la casa de uno, control sobre información personal, libertad para no ser vigilado, protección a la

reputación de uno, y protección contra investigaciones e interrogaciones.[23]

De esa orden de ideas, de primer momento, se puede desprender que la idea de privacidad puede ser entendida como un espectro individual de derechos a partir del cual se pueden conceptualizar otros tipos de derechos y libertades individuales que pueden ser dirigidos y ejercidos en diversas facetas de la vida tanto individual como social. Desde la más intrínseca —y quizá automática— expresión de vida que pueden tener los seres humanos, como lo es el pensamiento, hasta el ejercicio de defensa contra la intromisión de terceros en la protección contra investigaciones e interrogaciones.

Por otra parte, y en ese mismo sentido, se podría ubicar la idea de Ernesto Garzón Valdés, al establecer que los límites de la privacidad es algo que depende del contexto cultural y social[24] es decir, que las concepciones y convenciones de cualquier aspecto de la vida social que se tienen por hoy entendidas y respetadas, no significa que lo seguirán siendo en un futuro probablemente diferente al status actual en donde los entornos sociales, económicos, culturales, quizá diferentes a

---

[23] Solove, Daniel J., "Undertandig privacy" [en línea], *George Washington University Law School, Public Law & Legla Theory Research Paper Series*, paper núm. 420, 2008, disponible en: *http://ssrn.com/abstract=1127888*, consultado el 19 de julio de 2019.

Texto en idioma inglés: Privacy, however, is a concept in disarray. Nobody can articulate what it means. Currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations. [traducción libre].

[24] Garzón Valdés, Ernesto, *Lo íntimo, lo privado y lo público*, Cuadernillos de transparencia, México, Instituto Federal de Acceso a la Información Pública (IFAI), núm. 6, 2008, p. 17.

los de la actualidad, redefinan los espacios, las apreciaciones, las valoraciones y el entendimiento humano hoy por hoy fijado.

> La definición legal de lo privado y de los recursos para protegerlo cambian también con el tiempo porque cambian las ideas y cambian las formas de organización, cambia la tecnología con la que se puede vigilar, interferir o asegurar cada ámbito. Hoy hace falta, por ejemplo, legislar con respecto a las telecomunicaciones o al uso de la informática porque hay la posibilidad técnica de proteger, compartir o difundir una masa de información que nunca antes había estado disponible de ese modo. Aspectos de la vida familiar, la sexualidad o la medicina que antes estaban sancionados, como asuntos de interés público, que correspondían incluso al derecho penal, hoy se consideran puramente privados.[25]

También, aporta a este mismo orden de ideas, lo establecido en el manual que, con propósito del curso de introducción a la Ley General de protección de datos personales en posesión de sujetos obligados editó el INAI y en donde se establece que, "El derecho a la protección de los datos personales es distinto del derecho a la privacidad. Este último podría definirse como el derecho que todo individuo tiene a separar aspectos de su vida privada del escrutinio público. *Es un derecho complejo, difícil de definir, pues cada persona es quien decide qué aspectos de su vida personal hace del conocimiento de los demás*".[26]

---

[25] Escalante Gonzalbo, Fernando, *El derecho a la privacidad*, Cuadernillos de transparencia, México, Instituto Federal de Acceso a la Información Pública (IFAI), núm. 2, 2008, p. 9.

[26] Instituto Nacional de Acceso a la Información Pública y Protección de datos personales (INAI), "Introducción a la Ley General de protección de datos personales en posesión de sujetos obligados: manual del participante", México, 2017, disponible en: *http://www.ift.org.mx/sites/default/files/anexo_circular_10-18_manual_lgpdppso_acc.pdf*. [Las cursivas son propias], última fecha de consulta el 31 de octubre de 2019.

Con esta última aportación, en la perspectiva de un concepto de intimidad inacabado, flexible, subjetivo y moldeable, podemos llegar a la conclusión de que es un concepto que no podría ubicarse fijamente en el tiempo y permanecer como un convencionalismo estático e inerte, sino por lo contrario, que es un concepto flexible y adaptable a la evolución de la sociedad, de sus instituciones y principalmente de sus interpretaciones y sus defectos.

Por otra parte, existe otra serie de planteamientos sobre el término privacidad que pueden aglomerarse en un mismo sentido y que pueden ofrecer también una concepción más o menos similar que pudiera aportar mayor sentido al desarrollo del presente trabajo.

Así pues, en un primer momento, el diccionario de la Real Academia Española define a la privacidad como "ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión".[27] De este concepto, podemos rescatar la frase "derecho a proteger", lo que nos da pauta a pensar en la posibilidad de ejercicio de un derecho y anteponerlo frente a terceros, como esencia ontológica de cualquier derecho subjetivo.

En ese mismo tenor, ubicamos a Fernando Escalante Gonzalbo, quien señala que:

> …lo primero que conviene tener presente es que lo privado es una creación del Estado, mediante la ley. Se configura por un acto de autoridad. Eso implica que puede modificarse y que, en cada caso, debe darse una justificación, debe explicarse por qué razón esa materia no es objeto de interés público, de modo que los particulares pueden decidir al respecto con entera libertad.[28]

---

[27] Real Academia Española: diccionario de la lengua española [en línea], disponible en: *https://dle.rae.es/?id=UD4g0KW*, última fecha de consulta el 9 de julio de 2019.

[28] Escalante Gonzalbo, Fernando, *op. cit.,* nota 26, p. 17.

De estas palabras, podemos resaltar lo que el autor establece al señalar que lo privado es una creación del Estado y que es el mismo Estado quien pudiera, mediante un acto de autoridad, reconfigurar los espacios entendidos como parte de lo privado. Esta afirmación por parte del autor retoma especial atención puesto que en contraposición a los postulados por el grupo que podemos decir establece una inacabada concepción de la privacidad, en esta vertiente se da a entender que es precisamente el Estado quien en función de potestades y de las necesidades y prioridades colectivas, pudiera en determinado momento redimensionar los espacios públicos y aquellos que pueden ser entendidos como espacios privados.

Por último, José Luís Piñar Mañas, establece que "(…) lo que identifica por igual a los expresados tipos de privacidad es que en todos ellos el individuo debe poder controlar el nivel de interacción con los otros. La idea del control es la clave esencial de la privacidad, ocupa el papel central".[29]

En esta última posición, el autor hace mención sobre la posibilidad que tienen los individuos de controlar y disponer espacios que consigna como privados y poder hasta cierto punto, darles apertura para que exista interacción con los demás, centrando como idea primordial el control de la privacidad por la misma persona.

Es en esta última perspectiva, en esta concepción de la privacidad sobre la que se postula el objetivo central de este trabajo. Es decir, la posibilidad de que los alumnos, el cuerpo docente y el personal administrativo que ha cedido su información personal a cualquier institución educativa, puedan en determinado momento saber en dónde y cómo se encuentran sus datos personales, quién y

[29] Piñar Mañas, José Luis, "¿Existe privacidad?", en H. Cámara de Diputados, *Protección de datos personales: compendio de lecturas y compilación*, México, Tiro Corto Editores, 2010, p. 17, disponible en: *http://www.transparencia.udg.mx/sites/default/files/Protecci%C3%B3n%20de%20datos%20personales.%20Compendio%20de%20lecturas%20y%20legislaci%C3%B3n.pdf*, última fecha de consulta el 31 de octubre de 2019.

para qué se utilizan y cuáles son las garantías físicas, lógicas y administrativas en las que se encuentran depositada su información personal. Cerramos la anterior interrogativa con la siguiente más que constataría perspectiva:

> De todos los Derechos Humanos incluidos en los catálogos internacionales, *la privacidad es quizás el más difícil de definir.* Las definiciones de privacidad varían ampliamente de acuerdo al contexto y al medio. En muchos países, el concepto ha sido fusionado con el de protección de datos, el cual entiende a la privacidad en términos del manejo de la información personal.[30]

Es con esta última posición con la que coincidimos, puesto que como ya se pudo esgrimir párrafos anteriores, será el futuro contexto temporal, espacial y social el que determine y decrete las nuevas perspectivas con las cuales habrán de concebirse los conceptos que ahora son aceptados convencionalmente. La tecnología, se insiste, habrá de dar origen a la necesidad de reconfigurar, replantear y rediseñar lo hoy entendido y vivido.

1.2.2. Divergencia conceptual entre privacidad e intimidad

No es objetivo del presente trabajo adentrarse en honduras filosóficas o epistemológicas sobre las diferencias conceptuales entre privacidad e intimidad.[31]

---

[30] Cédric Laurant Consulting and Privacy, “Guía de privacidad para hispanoparlantes 2012” [en línea], Privacy International, p. 59, disponible en: *https://issuu.com/cedriclaurant/docs/120101-guia_privacidad_2012-clc_pi-c*. [Las cursivas son propias], última fecha de consulta el 31 de octubre de 2019.

[31] Sin embargo, se considera prudente verter el concepto de *intimidad* con la intención de que el lector pueda contar con los elementos conceptuales suficientes para poder contrastar las ideas que aquí se exponen. Para ello, se establece que la palabra *intimidad*, “da idea de algo interior, algo recóndito, profundo del ser y por lo oculto, escondido, de manera tal que podemos decir que se trata de un ámbito individual de existencia personal en el cual el sujeto decide su forma de ser y de estar, de verse él mismo, para gozar de su soledad o convivencia tranquila a

Sin embargo, se estima pertinente presentar los diversos planteamientos que al respecto se han encontrado con la finalidad de poder tener un poco más claro desde qué perspectiva en considerado en México la protección de la información personal.

En primer lugar, la SCJN emitió un criterio jurisprudencial al respecto estableciendo lo siguiente:

> **DERECHO A *LA PRIVACIDAD O INTIMIDAD*. ESTÁ PROTEGIDO POR EL ARTÍCULO 16, PRIMER PÁRRAFO, DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS.**
>
> Dicho numeral establece, en general, la garantía de seguridad jurídica de todo gobernado a no ser molestado en su persona, familia, papeles o posesiones, sino cuando medie mandato de autoridad competente debidamente fundado y motivado, de lo que deriva la inviolabilidad del domicilio, cuya finalidad primordial es el respeto a un ámbito de la vida privada personal y familiar que debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás, con la limitante que la Constitución Política de los Estados Unidos Mexicanos establece para las autoridades. En un sentido amplio, la referida garantía puede extenderse a una protección que va más allá del aseguramiento del domicilio como espacio físico en que se desenvuelve normalmente *la privacidad o la intimidad*, de lo cual deriva el reconocimiento en el

---

fin de encontrarse en aptitud de reflexionar, analizar, pensar, crear, trabajar, amar, soñar; en fin, para sentirse anímicamente dueño de sí y mantener su libertad como suprema aspiración humana". Celis Quintal, Marcos Alejandro, "La protección de la intimidad como derecho fundamental de los mexicanos" [en línea], en Cienfuegos Salgado, David y Macías Vázquez María Carmen (coords.), *Estudios en homenaje a Marcia Muñoz de Alba Medrano*. *Protección de la persona y derechos fundamentales*, México, 2006, disponible en: *https://dialnet.unirioja.es/servlet/autor?codigo=2032970*, última fecha de consulta el 31 de octubre de 2019.

> artículo 16, primer párrafo, constitucional, de un derecho a la intimidad o vida privada de los gobernados que abarca las intromisiones o molestias que por cualquier medio puedan realizarse en ese ámbito reservado de la vida.[32]

Del anterior criterio, podemos notar que la SCJN no hace distingo alguno entre los conceptos *privacidad* e *intimidad* al utilizar la conjunción disyuntiva "o" entre ambos conceptos, entendiéndose de esta manera que entre los mismos no existe diferencia y que ambos podrían tomarse en el mismo sentido, por lo que, siguiendo el sentido de este criterio, es en el artículo 16 de nuestra magna carta en donde se instituye el derecho a la privacidad o intimidad de los mexicanos.

En sentido diferente, es la misma Suprema Corte mexicana la que aporta otro criterio jurisprudencial que ofrece otros elementos interpretativos que alimentan la divergencia terminológica entre ambos conceptos, estableciendo lo siguiente:

> La vida se constituye por el ámbito privado reservado para cada persona y del que quedan excluidos los demás, mientras que la intimidad se integra con los extremos más personales de la vida y del entorno familiar, cuyo conocimiento se reserva para los integrantes de la unidad familiar. Así, *el concepto de vida privada comprende a la intimidad* como el núcleo protegido con mayor celo y fuerza porque se entiende como esencial en la configuración de la persona, esto es, la vida privada es lo genéricamente reservado y la intimidad -como parte de aquélla- lo radicalmente vedado, lo más personal; *de ahí que si bien*

[32] Tesis: 2a. LXIII/2008, Semanario Judicial de la Federación y su Gaceta, Novena Época, tomo XXVII, mayo de 2008, p. 229. [Las cursivas son propias], última fecha de consulta el 31 de octubre de 2019.

son derechos distintos, al formar parte uno del otro, cuando se afecta la intimidad, se agravia a la vida privada.[33]

De este otro criterio se puede observar que nuestro máximo tribunal hace una distinción entre ambos conceptos al establecer que ambos *son derechos distintos*, pudiéndose establecer que uno forma parte de otro estableciéndose una relación distintiva entre lo general y lo particular fijándose que, si en determinado momento se conculca uno de ellos, colateralmente se agravia al otro.

Así pues, podemos observar que derivado de los planteamientos en los dos criterios previamente establecidos emitidos por nuestro máximo tribunal de justicia, no se puede encontrar una clara distinción entre ambas concepciones concluyéndose de esta manera que existe una falta de unidad en las interpretaciones que al respecto se han emitido.

Bien es sabido que las manifestaciones y las consecuencias de los avances de la técnica aparecerán siempre en tiempos anteriores a los tiempos del derecho. En otras palabras, los avances tecnológicos surgen antes de los marcos jurídicos normativos aplicables a la técnica. Técnica que tendrá que ser puesta en práctica para poder con ello valorar y medir sus impactos y sus secuelas generándose de esta forma nuevos y desconocidos retos al derecho. “Las Tecnologías de la Información han transformado nuestras vidas, y nos hemos rendido ante ellas. Para el Derecho y para la Política esto significa nuevos retos, grandes y desconocidos retos”.[34]

---

[33] Suprema Corte de Justicia d la Nación, Primera Sala. Novena Época. Semanario Judicial de la Federación y su Gaceta. Tomo XXVI, julio de 2007. [Las cursivas son propias]

[34] Lefranc Weegan, Federico César, *Terra incógnita. Bases para una política criminal pro persona en la sociedad digital*, Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación (INFOTEC), México, 2015, p. 47, disponible en: *https://www.infotec.mx/work/models/infotec/biblioteca/25/25.pdf*, última fecha de consulta el 31 de octubre de 2019.

Estos sucesos se traen a colación al presente trabajo dado que este mismo escenario ha repercutido de la misma manera en el campo de la protección a la privacidad, generándose de esta forma que diferentes áreas del derecho se hayan tenido que reconfigurar y redimensionar en cuanto a sus alcances, sus propósitos y sus concepciones.

> *El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida. Nótese que se habla de la privacidad y no de la intimidad: Aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona —el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo—, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado. Y si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 de la Constitución y por las leyes que los desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo*.[35]

Como se puede apreciar, la aparición, aplicación, uso y explotación de las TIC ha transformado sobremanera la concepción terminológica que se ha tenido entre el derecho a la privacidad y el derecho a la intimidad. Se ha transformado de alguna manera que, hasta estos días, sigue siendo la raíz semántica para que sigan apareciendo diversas posturas conceptuales entre ambas palabras.

[35] Díaz Revorio, Francisco Javier, *op. cit.,* nota 21, p. 177.

Con todo lo esgrimido previamente, podemos hacer las consideraciones finales al presente apartado en el sentido de que hasta el momento no existe una clara distinción entre los conceptos de intimidad y privacidad; tampoco se tiene vislumbrado un modelo de interpretación jurídica que ayude a establecer determinantemente los límites entre una y otra.

Hasta el momento ni posturas filosóficas ni profundas interpretaciones jurídicas han ayudado al respecto, sin embargo, podría sostenerse, conforme a lo que aquí se ha venido planteando, que podemos ubicar al derecho a la protección de datos personales como un derecho originado a partir del concepto de privacidad, más que uno derivado del concepto de intimidad.

1.2.3 El derecho a la protección de la privacidad

Una vez ya expuesta la divergencia conceptual entre privacidad e intimidad y las diferentes posturas que al respecto se han esgrimido tanto por instituciones oficiales como por diferentes organizaciones y tratadistas especialistas en la materia, a continuación, se presenta la temática del derecho a la protección de la privacidad concebida en el seno de los órganos e instituciones rectores de la protección de los derechos humanos, tanto a nivel internacional como regional.

Así entonces, resulta primordial remitirnos a lo que se encuentra establecido en el artículo 12 de la Declaración Universal de los Derechos Humanos al señalar que “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”.[36]

Como puede observarse, en la composición de este artículo se utiliza el concepto *vida privada*, y no *privacidad*, situación que no debería causar mayor problemática conceptual, pues se considera que tanto gramatical como

[36] Declaración Universal de los Derechos Humanos, disponible en: *https://www.ohchr.org/en/udhr/documents/udhr_translations/spn.pdf*, fecha de consulta 20 de julio de 2019.

sustancialmente, expresan y pueden entenderse los mismos fines, la misma sustancia.

Por otra parte, el apartado 1 del artículo 17 del Pacto Internacional de Derechos Civiles y Políticos lo establece de la siguiente manera *"Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación".*[37]

Siguiendo esta misma perspectiva y concepción de la protección a la privacidad, el artículo octavo, numeral 1 del Convenio Europeo de Derechos Humanos, en el apartado relativo al derecho al respeto a la vida privada y familiar, se establece que "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia".[38]

Finalmente, en el entorno del sistema americano de protección de Derechos Humanos, en el llamado Pacto de San José relativo a protección de la honra y de la dignidad en el artículo 11 apartado 2, se establece que "Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación".[39]

Con todos estos precedentes, se hace suficiente constancia para concluir en que la protección a la información personal es considerada, al menos desde la perspectiva de los organismos internacionales en materia de derechos humanos, desde un enfoque de protección de la privacidad, y no a la intimidad, como es

---

[37] Pacto Internacional de Derechos Civiles y Políticos, disponible en: *http://www.corteidh.or.cr/tablas/3769.pdf*, última fecha de consulta el 20 de julio de 2019.

[38] Convenio Europeo de Derechos Humanos, disponible en: *https://www.echr.coe.int/Documents/Convention_SPA.pdf*, última fecha de consulta el 20 de julio de 2019.

[39] Convención Americana de Derechos Humanos, disponible en: *http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/D1BIS.pdf*, última fecha de consulta el 20 de julio de 2019.

señalada por diferentes tratadistas en la materia y sobre lo cual ya se ofreció una serie de planteamientos y disertaciones.

En ese mismo sentido la Constitución Política de los Estados Unidos Mexicanos instituye la protección de la privacidad de los mexicanos en el artículo 16, primer párrafo, al establecer que “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”.

Aunque expresamente no se hace referencia al concepto privacidad, los elementos descriptivos con que se formula tal artículo adoptan el núcleo esencial que soporta y da base a la protección a la privacidad y las relaciones y la convivencia entre los miembros familiares, espacios que no pueden no deben arbitrariamente ser violados o traspasados por cualquier tercero que así lo intentase, aun siendo representantes de la autoridad.

De esta forma es como podemos concluir, como se ha venido postulando a lo largo del presente trabajo, en que la protección de los datos personales es reflexionada y razonada como un núcleo de protección derivado del genérico llamado privacidad, y no tanto de intimidad, bien jurídico también protegido desde otros campos y perspectivas del derecho.

1.3 Las universidades públicas como sujetos obligados a la protección de datos personales de acuerdo con la legislación mexicana

La cesión de datos personales entre individuos a lo largo de la historia ha sido un constante y permanente ejercicio de acuerdos, tácitos o expresos, voluntarios o involuntarios. Sin embargo, hoy más que nunca esta situación se ha hecho más evidente y quizá más necesaria. La aceleración en todos los aspectos de la conducta de los seres humanos provoca que se busquen procesos más rápidos, eficientes y satisfactorios.

Muchos de esos procesos se basan en el intercambio de información personal en todas sus modalidades. Desde trámites ante entidades y organismos del gobierno, hasta chequeos rutinarios ante los expertos en medicina, los acuerdos se basan en la cesión, disposición y tratamiento de datos personales.

A partir de esto, podemos claramente constatar que son dos sectores o vertientes en donde la cesión de datos personales se hace evidente. Por una parte, se recaban datos personales en los organismos, entidades e instituciones representantes del sector público, y por otra, las personas de carácter privado que también recaban y tratan información personal dentro de sus procesos de control y gestión en sus modelos de negocios.

Para ello, en este apartado de ofrecerá lo que se concibe como universidad pública, ubicándose a estas dentro del sector público como también responsable en el tratamiento de datos personales.

1.3.1 Concepto de universidad pública

El INAI, siendo el órgano garante para la protección de datos personales tanto del sector público como el sector privado en México, emitió en fecha 4 de enero de 2018 un comunicado con relación a las instituciones educativas en donde, entre otras cosas, señala que:

> Las instituciones educativas deben garantizar el tratamiento adecuado de los datos personales de estudiantes, tutores de los alumnos y trabajadores. Cuando no cumplen con esta obligación, la población puede acudir al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), para hacer valer sus derechos y presentar las denuncias respectivas.[40]

[40] Comunicado del INAI de fecha 4 de enero de 2018, titulado: *Garantiza INAI a titulares el acceso a datos personales resguardados por instituciones educativas*, disponible en: *https://www.mugsnoticias.com.mx/noticias-del-dia/garantiza-inai-a-*

Con este antecedente, se ofrecen dos aportaciones en cuanto la conceptualización de universidad pública, esto dado que el objetivo del presente trabajo será aplicable precisamente a una institución educativa de nivel superior, teniendo en primer momento que:

> Una universidad pública es una institución de educación superior que existe para cumplir con el derecho ciudadano a la educación en todos sus niveles, de acuerdo a los conocimientos y la formación ciudadana que la sociedad define como necesarios; una universidad pública desarrolla la investigación que la nación necesita para aumentar sus conocimientos y enfrentar sus problemas; una universidad pública está comprometida a entregar a toda la comunidad del país el producto de su trabajo, extendiendo sus estudios y creaciones más allá de los límites de sus dependencias. Su pluralismo es una consecuencia necesaria del hecho de ser una universidad de todos. De aquí también deriva la transparencia de su gestión y las normas que rigen su convivencia interna.[41]

Derivado de lo anterior, podemos establecer que dado el fin primordial que persiguen estas instituciones, que es la importación de educación pública, como órgano público y controlado por dependencias del gobierno, tienen que apegarse a lo dispuesto y establecido a lo mandatado por las leyes orgánicas de la administración pública estatal ya sea a nivel nacional, o aplicable a cada entidad federativa.

Resulta válido hacer mención finalmente, de que, en las tareas de búsqueda y acopio de información para la elaboración del presente trabajo, se ha

---

titulares-el-acceso-a-datos-personales-resguardados-por-instituciones-educativas/, última fecha de consulta el 31 de octubre de 2019.

[41] Baño, Rodrigo, "¿Qué es una Univerisidad Pública?, Universidad de Chile, Facultad de Ciencias Sociales, disponible en *http://www.facso.uchile.cl/noticias/67245/que-es-una-universidad-publica*, última fecha de consulta 21 de julio de 2019.

encontrado con poca información en relación a los deberes y compromisos de las universidades públicas como sujetos obligados a la protección de datos personales de las personas que de alguna u otra manera disponen o ceden su información personal para los fines mismos de este tipo de instituciones. Se espera que el presente represente un mensaje a aquellos que quisieran ampliar la investigación y desarrollo de trabajos relacionados al tema que hoy nos ocupa, la protección de datos personales en las instituciones educativas de nivel superior en México.

1.3.2 Concepto de sujeto obligado

Antes de dar inicio a este apartado, se considera pertinente hacer el señalamiento de que tanto el derecho a la protección de datos personales como el derecho al acceso a la información pública han tenido relativa aparición e inclusión en el orden jurídico mexicano, no obstante su aparición y consolidación con anterioridad en otras regiones del mundo, llegándose a considerar, incluso, que el primero es una especie de contrapeso del segundo.

> A partir de 2006, en el contexto de la reforma al artículo 6 de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia y acceso a la información, se hace la primera referencia constitucional al derecho a la protección de datos personales, pero sin regularlo sustancialmente, reiterando el papel de este derecho como contrapeso del derecho de acceso a la información.[42]

Este pequeño preámbulo da pie para abordar la conceptualización que sobre *sujeto obligado* se tiene, puesto que al tratar de encontrar una concepción

[42] Iniciativa con proyecto de decreto por la que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Salón de Sesiones del Pleno del Senado de la República, 30 de abril de 2015, disponible en: *http://www.senado.gob.mx/comisiones/gobernacion/docs/proteccion_datos/Iniciativa.pdf*, última fecha de consulta el 31 de octubre de 2019.

emitida por expertos tratadistas en la materia, solamente se remite a los diferentes catálogos que al respecto se han establecido en las leyes generales tanto de acceso a la información pública como la de protección de datos personales en posesión de sujetos obligados, resumiéndose, por ambos cuerpos normativos, *que ambos derechos vincula a quienes cumplan funciones públicas, presten servicios públicos o ejecuten, en nombre del Estado, recursos públicos*, estipulando ambos cuerpos normativos lo siguiente:

1) Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Artículo 1. (…)

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

2) Ley General de Transparencia y Acceso a la Información Pública.

> Artículo 23. Son sujetos obligados a transparentar y permitir el acceso a su información y proteger los datos personales que obren en su poder: 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 los ámbitos federal, de las Entidades Federativas y municipal.

Finalmente, y en ese mismo tenor, la página oficial del órgano garante del Estado de México, el Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios (Infoem),[43]

[43] Para saber a detalle cuales son los organismos, dependencias, entidades, instituciones o personas jurídico-colectivas adscritas a cada sujeto obligado del

hace la siguiente clasificación de los sujetos obligados a la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de México y Municipios. Así entonces:

> Artículo 3. Son sujetos obligados por esta Ley:
> I. El Poder Ejecutivo.
> II. El Poder Legislativo.
> III. El Poder Judicial.
> IV. Los Ayuntamientos,
> V. Los Órganos y Organismos Constitucionales Autónomos.
> VI. Los Tribunales Administrativos.
> VII. Los Partidos Políticos.
> VIII. Los Fideicomisos y Fondos Públicos.

En ese sentido, como se desprende de los anteriores listados relativos a la normatividad en la materia y atendiendo al fin último de este tipo de leyes que establece que son *sujetos obligados* aquellas dependencias, organismos, entidades e instituciones que de alguna u otra manera llevan a cabo *funciones públicas, presten servicios públicos o ejecuten, en nombre del Estado, recursos públicos*, son las universidades públicas las que derivado de su propia naturaleza, actualizan dicha máxima, sometiéndose ineludiblemente a la observancia de estos cuerpos normativos.

1.4 Consideraciones finales al capítulo uno

La elaboración del presente capítulo ha tenido como objetivo principal el de proveer los conceptos fundamentales relativos al derecho a la privacidad y protección de datos personales en el entorno de las universidades públicas como sujetos obligados a observar la normativa aplicable a la materia, y consecuentemente con ello, permitir que aquellos que den lectura al presente trabajo puedan tener los elementos conceptuales fundamentales de la temática y

---

Gobierno Estatal del Estado de México, acceder a la página oficial, disponible en: *https://www.infoem.org.mx/*, última fecha de consulta el 31 de octubre de 2019.

permitirles una lectura más asimilable y no tan tortuosa derivado de los términos técnicos relativos a la materia.

Por otra parte, se pudo hacer constancia de que los conceptos aquí presentados, aun perteneciendo a la misma materia y temática, son esgrimidos con rasgos y características distintos entre ellos. Un ejemplo muy claro al respecto es la apreciación que se tiene con relación a la protección de los datos personales, puesto que por un lado se considera como parte del derecho a la intimidad, pero por otro lado se toma como parte del derecho a la privacidad.

También es de concluir a partir del presente capítulo, que, después de una ardua búsqueda por encontrar definiciones del concepto *sujeto obligado*, no se pudo encontrar tales referencias, teniéndose que remitir únicamente a los diferentes catálogos de sujetos obligados que las páginas oficiales de los gobiernos estatales presentan, aunado a lo establecido en las leyes de acceso a la información pública y de protección de datos personales, como en la ley del Estado de México en materia de protección de datos en posesión de sujetos obligados.

Capítulo 2

Marco jurídico internacional, nacional y local (Estado de México) sobre el derecho a la protección de datos personales

Capítulo 2. Marco jurídico internacional, nacional y local (Estado de México) sobre el derecho a la protección de datos personales

Una vez hecha la descripción del marco teórico conceptual en el capítulo que antecede, a continuación, se presenta el marco jurídico aplicable a la temática de la protección de datos personales en México, con la intención de brindar al lector el contexto normativo observable en dicha materia por los sujetos obligados catalogados con acuerdo a la Ley local de protección de datos.

Para ello resulta importante considerar que, con acuerdo a la naturaleza jurídica de la UPTex, objeto de este trabajo, es una institución dependiente del gobierno del estado de México actualizándose de esta forma la obligación de la institución de acatar lo establecido en dicha normatividad.

Este escenario resulta ser de primordial atención puesto que, con acuerdo a la ley previamente referida, son precisamente este tipo de instituciones públicas las que, en atención a su propia ordenación jurídica, se configura como sujeto obligado a atender y observar las disposiciones legales aplicables.

Una obligación que tienen este tipo de instituciones por ley establecida es la de contar con un SGDP diseñado, implementado, aplicado, gestionado y evaluado de acuerdo a las propias y especiales características internas de la institución, obligación que de no ser satisfecha, podría tener como consecuencias además de las sanciones previstas en ley, un descrédito por parte de la sociedad al conocer las deficiencias y quizá falta de seriedad por esta institución en relación a sus procesos internos de control y gestión de datos personales.

Una vez descrito el marco normativo aplicable al presente subtema, el lector podrá contar con los elementos tanto teóricos —ofrecidos en el primer capítulo—, como jurídicos para que se pueda concebir la importancia de contar con denominado sistema dentro de la institución.

Para ello se analizarán instrumentos internacionales en materia de protección de datos personales, así como las leyes tanto de carácter nacional y,

necesario y obligatoriamente, la ley aplicable al Estado de México, no sin olvidar la parte técnica aplicable a la materia que se puede encontrar en diversos documentos de estandarización de procesos de gestión de datos personales.

2.1 El surgimiento del derecho a la protección de datos personales

Como al inicio del primer capítulo de este trabajo, se vuelve a mencionar al indetenible y permanente avance de la ciencia y de la tecnología como fuente generadora de re-concepciones, re-planteamientos y re-diseños de la actual vida social en muchas de sus diferentes manifestaciones, escenario que se manifiesta no solamente a escala nacional o regional, sino también con incidencias y expresiones de magnitud internacional.

En ese sentido, parece haber entre los tratadistas expertos en la materia del derecho a la protección de datos personales una generalizada percepción sobre que son el desarrollo, la evolución y sobre todo aplicación de las TIC —como parte del espectro de la ciencia en general— el campo de las ciencias en donde surgen y se manifiestan trascendentales expresiones tecnológicas teniéndose con ello, consecuente e inevitablemente, un impacto en los actuales esquemas jurídicos dentro de los cuales se formula la conducta social. “El impacto de las tecnologías de la información y de la comunicación (TIC) en el desarrollo de la sociedad actual es innegable, jugando un rol transcendental que se manifiesta de forma transversal no tan solo en los aspectos culturales y sociales de esta, sino también en sus aspectos económicos y políticos y, en lo que aquí más interesa, también jurídicos”.[44]

[44] Barinas Ubiñas, Désirée, “El impacto de las Tecnologías de la Información y de la Comunicación en el derecho a la vida privada: las nuevas formas de ataque a la vida privada”, *Revista Electrónica de Ciencia Penal y Criminología*, núm. 15-09, p. 2, septiembre de 2013, disponible en: *http://criminet.ugr.es/recpc/15/recpc15-09.pdf*, fecha de consulta 10 de agosto de 2019.

Así pues, como se constata en la aportación previa, la evolución de las denominadas TIC, y más concretamente su puesta en práctica, se insiste, conllevan a que paralela e indefectiblemente se tengan que replantear las actuales estructuras socio-políticas, económicas y jurídicas, desde otras perspectivas y con muchas interrogantes al respecto, situación que merece ser observada con base en otros estados de atención y otros estados de crítica, desde otros espacios y con origen en otras preocupaciones tanto a nivel macro y micro social e incluso a niveles de lo que se puede llegar a considerar como lo más íntimo del ser humano, como lo pueden ser las emociones:

> Este derecho, consecuencia del desarrollo tecnológico y el creciente almacenamiento de información relativa a la persona, así como la inmersión cada vez mayor de la misma y de la propia sociedad a (*sic*) tenido que ir ampliando sus directrices, ya no sólo dentro de su contexto de los sentimientos, emociones, del hogar, de los papeles, la correspondencia, las comunicaciones telefónicas, videovigilancia, etcétera, sino que además, hoy, es necesario su reconocimiento, y más aún, el establecimiento de mecanismos de protección que puedan hacer frente a su uso y manejo.[45]

Estos fenómenos sociales de relativa aparición han generado inquietudes e interrogantes que, como se observa en la aportación anterior, hacen necesario que se piensen y generen mecanismos jurídicos de protección ante este tipo de expresión técnica con base en el modelo del masivo almacenamiento y tratamiento de información relativa a las personas. Tanto resultan ser así

---

[45] García González, Aristeo, “La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado”, Boletín Mexicano de Derecho Comparado, nueva serie [en línea], año XI, núm. 120, septiembre-diciembre, 2007, México, Instituto de Investigaciones Jurídicas de la UNAM, p. 751, disponible en *http://transparencia.udg.mx/sites/default/files/La%20protecci%C3%B3n%20de%20datos%20personales%20derecho%20fundamental%20del%20siglo%20XXI.%20un%20estudio%20comparado.pdf*, última fecha de consulta el 1 de agosto de 2019.

apreciadas estas inquietudes, que incluso ya han comenzado a aparecer en el actual sistema jurídico instrumentos de protección jurídica enfocados al derecho, por ejemplo, a la cancelación[46] de información personal.

> Precisamente es en el derecho a la protección de datos personales en donde podemos encontrar las respuestas ante los retos que ha ido planteando el avance del desarrollo tecnológico, herramientas como el derecho al olvido (derecho de cancelación) han ido equilibrando los intereses en presencia de situaciones como las descritas. Así ante esa memoria indeleble que pueden significar diversas plataformas en Internet, ahora es posible ejercer un derecho al olvido que permite eliminar de las mismas, cualquier información que le pertenezca a una persona y de ese modo garantizar el poder de disposición sobre la información personal.[47]

Como se puede apreciar en el anterior extracto de la entonces iniciativa de la ya ahora en vigencia Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en México, esta misma inquietud fue observada y

---

[46] El derecho a la cancelación de datos personales es parte de lo que entre los tratadistas se ha denominado el derecho a la autodeterminación informativa, comprendiendo además del derecho a la cancelación, el derecho al acceso, el derecho a la rectificación y el derecho a la oposición de datos personales, conocido por sus siglas, como los derechos ARCO. Para un mayor acercamiento al tema de los derechos ARCO como mecanismos de protección dentro del llamado derecho a la autodeterminación informativa, remitirse a: Arroyo Kalis, Juan Ángel, "*Habeas data:* elementos conceptuales para su implementación en México", México, Instituto de Investigaciones Jurídicas de la UNAM, disponible en: *https://archivos.juridicas.unam.mx/www/bjv/libros/10/4633/4.pdf*, última fecha de consulta el 31 de octubre de 2019.

[47] Iniciativa con proyecto de decreto por la que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, *op. cit*., nota 44, p. 2.

discutida con la misma zozobra en nuestro país al igual que en muchos países de otras latitudes.

Ahora bien, la manifestación de este tipo de inquietudes no ha sido ni debe ser privativa del sector público y de sus organismos y entidades que lo integran y conforman, sino debe también, en la misma escala y magnitud, ser observado en el sector privado dado las propias características de muchos —sino es que la totalidad- de sus procesos internos de administración y de gestión de información que ostentan y manipulan.

> Ahora, con el tratamiento, la recolección, el almacenamiento de informaciones que antes sólo podía formar parte de la vida íntima de cada ser humano —o bien, era conocido por un mínimo sector—, ha ido variando paulatinamente su entorno y estructura. Esto es, los datos personales de toda persona se han convertido en una práctica habitual de control y almacenamiento por parte de los sectores tanto públicos como privados.[48]

Con todo lo hasta aquí presentado se puede llegar a hacer una conclusión al presente apartado señalando que, aunque a lo largo de la historia han existido manifestaciones e inquietudes por mantener y proteger aspectos privados de las personas, no ha sido sino hasta en las últimas del siglo XX, y aún más en las primeras décadas del siglo actual en donde, como consecuencia del extraordinario desarrollo de las TIC, se ha manifestado una creciente y patente preocupación por construir e implementar mecanismos jurídicos y normativos de protección a la privacidad de las personas como consecuencia del manejo y gestión de los datos personales en posesión de organizaciones e instituciones tanto del sector público como del privado.

> A fin de equilibrar las fuerzas entre un individuo y aquellas organizaciones –públicas o privadas- que recaban o colectan datos sobre tal individuo, surge en Europa el concepto de la protección de datos personales.

[48] García González, Aristeo, *op. cit*, nota 49, p. 745.

(…)

> Bajo el concepto de protección de datos personales, el titular (o dueño) de dichos datos es el propio individuo. En naciones avanzadas, la protección de datos personales es quizá el más nuevo de los derechos que goza un ciudadano.[49]

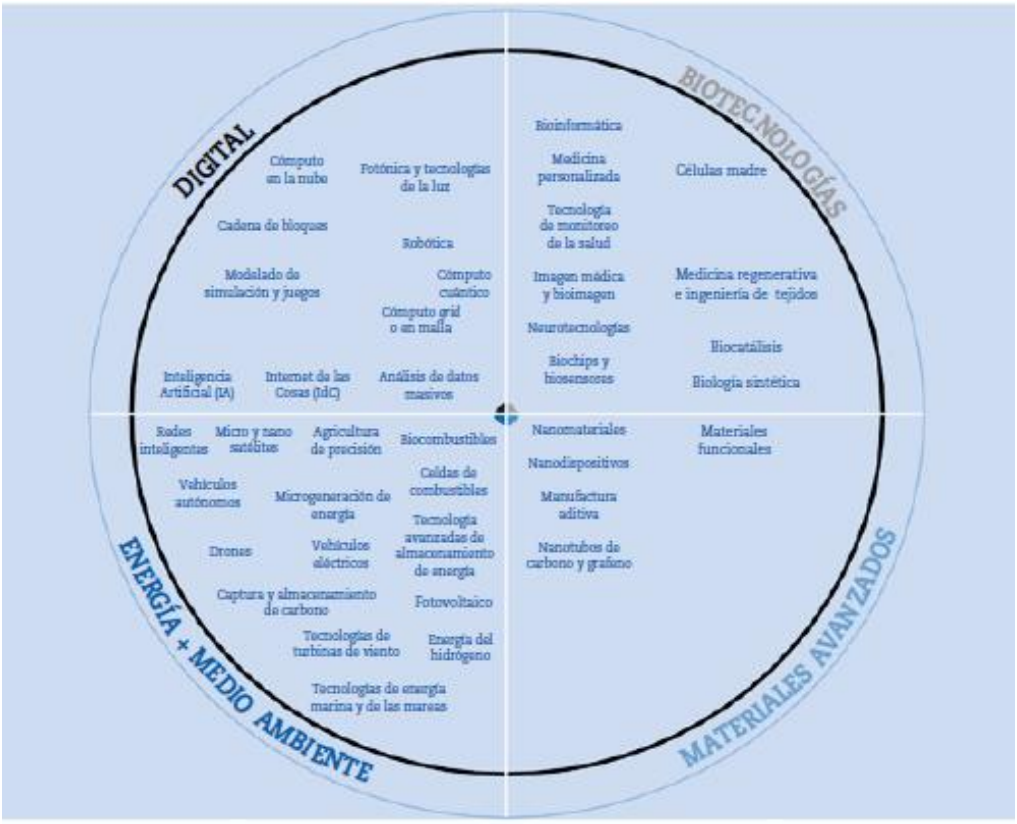
Teniendo en perspectiva la misma tendencia del abrupto e incesante desarrollo y aplicación de la técnica, puede resultar sensato pensar en que las décadas que están por presentarse traerán consigo colateralmente nuevos y significantes retos y desafíos a la protección de la privacidad y a la protección de la información personal.

En el material, “Perspectivas de la OCDE en ciencia, tecnología e innovación en América Latina”,[50] esta organización mapea 40 tecnologías clave y emergentes para el futuro, exponiéndolo de la siguiente manera:

Figura 1. 40 tecnologías clave y emergentes para el futuro.

[49] Presentación al libro “Protección de datos personales. Compendio de lecturas y legislación”, México, Tiro Corto Editores, 2010.

[50] OCDE, “Perspectivas de la OCDE en ciencia, tecnología e innovación 2016 (Extractos): América Latina”, París, OCDE, disponible en: *https://www.oecd-ilibrary.org/docserver/9789264303546-es.pdf?expires=1565822308&id=id&accname=guest&checksum=C0FDBAEEB11CCBD61FE752DFCC735E79*, última fecha de consulta el 31 de octubre de 2019.



Fuente: Perspectivas de la OCDE en ciencia, tecnología e innovación en América Latina.

Así pues, como se puede apreciar en la figura previa, específicamente en el cuadrante de la tecnología digital, varias de estas fundamentan sistemáticamente sus esquemas operacionales a partir del uso masivo de información de índole personal —como el caso del internet de las cosas[51] (IdC)— que seguirá, quizá

[51] Página oficial de Wikipedia, disponible en *https://es.wikipedia.org/wiki/Internet_de_las_cosas#Definici%C3%B3n_original*, última fecha de consulta el 29 de agosto de 2019. El internet de las cosas (en inglés, Internet of Things, abreviado IoT; IdC, por sus siglas en español) es un concepto que se refiere a una interconexión digital de objetos cotidianos con internet. Es, en definitiva, la conexión de internet más con objetos que con personas. También se suele conocer como internet de todas las cosas o internet en las cosas. Si los objetos de la vida cotidiana tuvieran incorporadas etiquetas de

inevitablemente, manteniendo al derecho a la protección de datos personales en estado de alerta y atención para poder de alguna manera crear y establecer mecanismos jurídicos de control e intervención en caso de violaciones al derecho a la privacidad y protección de la información personal.[52]

2.2 Contexto internacional del derecho a la protección de datos personales

Como se ha venido planteando a lo largo del presente trabajo, la protección de datos personales es un fenómeno jurídico con repercusiones no solo a nivel nacional o regional sino también a escala internacional. Y es precisamente este mismo contexto, la inquietud a escala mundial de la protección de la información personal, la que hace que este tema sea abordado y tratado desde diferentes foros y organizaciones internacionales preocupados por la promoción y el desarrollo del derecho a la protección de datos.

A continuación, se presentan a manera de ejemplo tres instrumentos en materia de protección de datos personales emitidos por diferentes organizaciones y foros internacionales que manifiestan y exponen dicha preocupación, siendo el primero de ellos la Organización para la Cooperación y Desarrollo Económicos.

---

radio, podrían ser identificados y gestionados por otros equipos de la misma manera que si lo fuesen por seres humanos,

[52] Algunos de los peligros y amenazas de la cada día mayor intrusiva tecnología en el desarrollo del denominado internet de las cosas, son 1) Identificación; 2) Localización y rastreo; 3) Perfilamiento; 4) Interacción y presentación pública de información privada; 5) Transiciones del ciclo de la vida; 6) Ataque al inventario, y 7) Enlaces. Para mayor detalle al respecto, Ziegeldorf, Jan Henrik, García Morchon, Oscar y Wehrle, Klaus, “Privacy in the Internet of Things: Threats and Challenges”, *Security and Communication Networks*, núm, 7, vol. 12, 2014, disponible en *https://arxiv.org/ftp/arxiv/papers/1505/1505.07683.pdf*, [Traducción libre], última fecha de consulta el 29 de agosto de 2019.

2.2.1 Las directrices de la Organización para la Cooperación y Desarrollo Económicos (OCDE)

La OCDE, de acuerdo a su página oficial, es una organización internacional que agrupa a 36 países miembros, de los cuales México es integrante desde mayo de 1994 y que tienen como misión "promover políticas que mejoren el bienestar económico y social de las personas alrededor del mundo… ofrecer un foro donde los gobiernos puedan trabajar conjuntamente para compartir experiencias y buscar soluciones a los problemas comunes… y fijar *estándares internacionales* dentro de un amplio rango de temas de políticas públicas". [53]

Como puede ser observado, uno de los objetivos que esta organización se ha establecido como misión es la fijar *estándares internacionales* que pueden ser considerados como *instrumentos no obligatorios* y que tienen como finalidad "ayudar a los gobiernos a fomentar la prosperidad y a luchar contra la pobreza a través del desarrollo económico, la estabilidad financiera, el comercio, la inversión, la tecnología, la innovación y la cooperación para el desarrollo".[54]

Con ese propósito, el de unificar y fijar criterios internacionales con miras a desarrollar la prosperidad internacional y luchar contra la pobreza, la desigualdad económica y promover y fomentar un comercio justo y el desarrollo de la tecnología, es que, en el año de 1980, actualizadas en el año 2013, esta organización emite las "Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales",[55] las cuales fueron formuladas en cinco apartados, siendo los siguientes:

---

[53] Sitio oficial de la Organización para la Cooperación y Desarrollo Económicos (OECD), disponible en: *https://www.oecd.org/centrodemexico/laocde/*, [Las cursivas son propias], última fecha de consulta el 13 de agosto de 2019.

[54] *Idem*.

[55] Las directrices sobre protección de la privacidad y flujos transfronterizos de datos personales ("directrices de privacidad") fueron adoptadas como una recomendación del Consejo de la OCDE apoyando los tres principios que aglutinan a los países de la OCDE: democracia pluralista, respeto de los derechos

1. Generalidades;
2. Principios básicos de aplicación nacional;
3. Principios básicos de aplicación internacional: restricciones en el libre flujo y la legitimidad;
4. Implantación nacional, y
5. Cooperación internacional.

Así entonces, se han considerado a la Directrices como “el primer instrumento supranacional que analiza el derecho a la protección de datos personales… las cuales se han utilizado a lo largo de los años en un gran número de instrumentos de regulación nacional, o de autorregulación, y todavía se usan ampliamente en los sectores público y privado”.[56]

Estas directrices a pesar de haber sido concebidas y diseñadas para ser aplicadas en el sector privado, como instrumentos reguladores del comercio internacional entre los países que integran la organización, no deja de ser un referente de primer nivel que ha merecido ser analizado y adaptado a las posteriores legislaciones en materia de protección de datos personales en muchos países como el caso de México, puesto que como se manifiesta en referido documento, los países miembro de la OCDE tienen un interés común en proteger

---

humanos y economías de mercado abiertas. Se hicieron efectivas el 23 de septiembre de 1980. Disponible en: *https://www.oecd.org/sti/ieconomy/15590267.pdf*, última fecha de consulta el 31 de octubre de 2019.

[56] Millán Gómez, Agustín, “Reconocimiento normativo del derecho a la protección de datos personales en el ámbito internacional”, *en Retos de la protección de datos personales en el sector público* [en línea], México, Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal (InfoDF), p. 26, disponible en: *http://www.infodf.org.mx/comsoc/campana/2012/LIbrodatosPweb.pdf*, última fecha de consulta el 31 de octubre de 2019.

la intimidad y las libertades individuales, y en reconciliar los valores fundamentales en oposición, tales como la intimidad y la libre circulación de información.

2.2.2 Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en los países de la OEA

Otro organismo internacional que ha mostrado preocupación por la protección de la privacidad y los datos personales, ahora desde una perspectiva regional o continental, es la OEA que se constituye como el principal foro gubernamental político, jurídico y social que reúne a las 35 naciones independientes del continente.

Este organismo, de acuerdo con su documento de creación, que es la Carta de la OEA, estipula en el artículo 1 que "Los Estados americanos consagran en esta Carta la organización internacional que han desarrollado para lograr un orden de paz y de justicia, fomentar su solidaridad, robustecer su colaboración y defender su soberanía, su integridad territorial y su independencia…".[57]

En ese sentido, la página oficial de este organismo continental establece que "Para lograr sus más importantes propósitos, la OEA se basa en sus principales pilares que son la democracia, los *derechos humanos*, la seguridad y el desarrollo".[58] Así entonces, y dado que la protección a la privacidad y la protección de datos personales es considerada por muchos tratadistas como un derecho fundamental,[59] la actuación de este organismo deberá de conducirse teniendo

[57] Carta de la organización de los Estados Americanos. Disponible en: *http://www.oas.org/es/sla/ddi/tratados_multilaterales_interamericanos_A-41_carta_OEA.asp*, última fecha de cosnulta el 31 de octubre de 2019.

[58] Disponible en: *http://www.oas.org/es/acerca/quienes_somos.asp*, última fecha de consulta 15 de agosto de 2019. [Las cursivas son propias].

[59] Dado no ser el objetivo principal del presente trabajo el dilucidar las diferencias filosóficas y ontológicas entre los conceptos derechos humanos y derechos fundamentales, se aclara que sólo para efectos del presente trabajo se utilizarán ambos términos indistintamente no haciendo entre ellos distingo alguno.

como propósito el velar y promover los derechos fundamentales de las personas, siendo concretamente en este caso, el derecho fundamental a la protección de datos personales.

Así pues, el 9 marzo de 2012 por medio de la Resolución CJI/RES. 186 (LXXX-O/12) emitida por el mismo organismo, se hace la propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas, mismos principios que tendrían como finalidad "establecer un marco para salvaguardar los derechos de la persona a la protección de los datos personales y a la autodeterminación en lo que respecta a la información. Los principios se basan en normas reconocidas a nivel internacional. Su intención es proteger a las personas de la recopilación, el uso, la retención y la divulgación ilícitos o innecesarios de datos personales".[60] Siendo tales principios los siguientes con breves explicaciones esgrimidas en la misma declaración:

Principio uno: propósitos legítimos y justos;

No deben recopilarse datos sobre personas excepto en las situaciones y con los métodos permitidos o autorizados por ley y (por lo general) deben darse a conocer a las personas afectadas en el momento en que se recopilen.

Principio dos: claridad y consentimiento;

Se basa en el concepto de la "autodeterminación en lo que respecta a la información" y, en particular, en dos conceptos que gozan de amplio reconocimiento a nivel internacional: el principio de "transparencia" y el principio de "consentimiento".

Principio tres: pertinencia y necesidad;

La exactitud, la pertinencia y la necesidad son principios cruciales de la protección de datos y la privacidad personal. Desde luego, sus requisitos deben evaluarse en relación con el contexto específico en el cual se recopilen, usen y

[60] Informe del Comité Jurídico Interamericano de la OEA sobre privacidad y protección de datos personales, de fecha 26 de marzo de 2016, disponible en: *http://www.redipd.es/documentacion/otrosdocumentos/common/Informe_CJI-doc_474-15_rev2_26_03_15.pdf*, última fecha de consulta el 15 de agosto de 2019.

divulguen los datos. Las consideraciones contextuales incluyen qué datos particulares se recopilan y con qué fines.

Principio cuatro: uso limitado y retención;

En este principio se enuncian dos premisas fundamentales con respecto a la retención de datos personales:

1) deben mantenerse y utilizarse de una manera legítima que no sea incompatible con el fin para el cual se hayan recopilado (lo cual se denomina a veces el “principio de finalidad” o “limitación del propósito”) y;

2) no deben mantenerse más del tiempo necesario para su propósito y de conformidad con la legislación nacional correspondiente.

Principio cinco: deber de confidencialidad;

Este deber requiere que el controlador de datos se cerciore de que no se proporcionen tales datos (ni se pongan a disposición por otros medios) a personas o entidades excepto con el conocimiento o consentimiento de la persona afectada, en consonancia con las expectativas razonables de la persona afectada o por mandato de la ley.

Principio seis: protección y seguridad;

De acuerdo con este principio, los controladores de datos tienen el deber claro de tomar las medidas prácticas y técnicas que sean necesarias para proteger los datos personales que obren en su poder o bajo su custodia (o de los cuales sean responsables) y cerciorarse de que tales datos personales no sean objeto de acceso, pérdida, destrucción, uso, modificación o divulgación excepto con el conocimiento o consentimiento de la persona o de otra autoridad legítima.

Principio siete: fidelidad de la información;

Cuando se recopilan datos personales y se los retiene para seguir usándolos (en vez de usarlos una sola vez o durante períodos cortos), el controlador de datos tiene la obligación de tomar medidas para que los datos se mantengan actualizados y sean exactos en la medida de lo necesario para los fines para los cuales se hayan recopilado y se usen.

Principio ocho: acceso y corrección;

Las personas deben tener derecho a saber si los controladores de datos tienen datos personales relacionados con ellas. Deben tener acceso a esos datos a fin de que puedan impugnar su exactitud y pedir al controlador de datos que modifique, revise, corrija o elimine los datos en cuestión. Este derecho de acceso y corrección es una de las salvaguardias más importantes en el campo de la protección de la privacidad.

Principio nueve: información sensible;

En ciertas circunstancias, podría considerarse que estos datos merecen protección especial porque, si se manejan o se divulgan de manera indebida, darían lugar a una intrusión profunda en la dignidad personal y el honor de la persona afectada y podrían desencadenar una discriminación ilícita o arbitraria contra la persona o causar un riesgo de graves perjuicios para la persona.

Principio diez: responsabilidad;

La protección efectiva de los derechos individuales de protección de la privacidad y de los datos se basa tanto en la conducta responsable de los controladores de datos como en las personas y en las autoridades gubernamentales del caso. Los sistemas de protección de la privacidad deben reflejar un equilibrio apropiado entre la reglamentación gubernamental y la implementación efectiva por aquellos que tienen responsabilidad directa por la recopilación, el uso, la retención y la difusión de datos personales.

Principio once: flujo transfronterizo de información y responsabilidad,

En el mundo moderno de rápidos flujos de datos y comercio transfronterizo, es cada vez más probable que las transferencias de datos personales crucen fronteras nacionales. Sin embargo, la reglamentación que existe actualmente en diversas jurisdicciones nacionales varía en cuanto al fondo y al procedimiento. En consecuencia, existe la posibilidad de confusión, conflictos y contradicciones.

Principio doce: publicidad de las excepciones.

Proteger los intereses en materia de privacidad de las personas (los ciudadanos y otros) es cada vez más importante en un mundo donde se recopilan ampliamente datos sobre personas, se los difunde con rapidez y se los almacena

durante mucho tiempo. La finalidad de estos principios es conferir a las personas los derechos básicos que necesitan para salvaguardar sus intereses.

Siendo la protección de los derechos humanos unos de los pilares fundamentales con base a los cuales la OEA se ha concebido, los anteriores principios han de ser reconocidos y considerados por todas las instituciones y organizaciones de los países miembro que de alguna u otra forma hacen del tratamiento de datos personales un proceso fundamental en la búsqueda y obtención de sus propósitos fundamentales, ya sean del sector privado o del sector público, como el caso de la universidades públicas en México y en este caso en concreto, de la UPTex que además de verse obligado a observar la legislación local y general en la materia, debe de orientar sus procesos institucionales con base a principios y esquemas como el que la OEA en este caso ha emitido.

2.2.3 Los estándares de Protección de Datos Personales de la RIPD

Finalmente, desde un enfoque intercontinental, la RIPD, integrada por los países de Andorra, Argentina, Chile, Colombia, Costa Rica, España, Perú, Portugal y Uruguay y de la cual México es integrante desde 2003, que:

> Se configura desde sus orígenes como un foro integrador de los diversos actores, tanto del sector público como privado, que *desarrollen iniciativas y proyectos relacionados con la protección de datos personales en Iberoamérica*, con la finalidad de fomentar, mantener y fortalecer un estrecho y permanente intercambio de información, experiencias y conocimientos entre ellos, así como promover los desarrollos normativos necesarios para garantizar una regulación avanzada del derecho a la protección de datos personales (…), tomando en consideración la necesidad del continuo flujo de datos entre países que tienen diversos lazos en común y una preocupación por este derecho.[61]

[61] Sitio oficial de la RIPDP, disponible en *http://www.redipd.es/la_red/Historia/index-ides-idphp.php*, última fecha de consulta el 16 de agosto de 2019.

Como lo podemos apreciar, es también en este tipo de foros intercontinentales en donde se generan oportunidades para habilitar espacios y canales de comunicación y poder de esta manera desarrollar iniciativas y proyectos relacionados con la materia de la protección de datos personales, situación que, con acuerdo al artículo 1 del reglamento de la RIPD, tendrá como uno de sus objetivo principales, "promover políticas, tecnologías y metodologías que permitan garantizar el *derecho fundamental a la protección de datos personales*".[62] Por ello es que la RIPD emite los Estándares de Protección de Datos Personales, los cuales tienen una serie de objetivos, siendo los que destacan, a efectos del presente trabajo, los siguientes:

- Establecer un conjunto de principios y derechos comunes de protección de datos personales que los Estados Iberoamericanos puedan adoptar y desarrollar en su legislación nacional, con la finalidad de contar con reglas homogéneas en la región.
- Garantizar el efectivo ejercicio y tutela del derecho a la protección de datos personales de cualquier persona física en los Estados Iberoamericanos, mediante el establecimiento de reglas comunes que aseguren el debido tratamiento de sus datos personales.
- Facilitar el flujo de los datos personales entre los Estados Iberoamericanos y más allá de sus fronteras, con la finalidad de coadyuvar al crecimiento económico y social de la región.

Como claramente se puede observar, las tres organizaciones —de índole internacional, regional e intercontinental— han plasmado e instituido en sus documentos base la preocupación de la protección de la privacidad y los datos personales desde el enfoque de los derechos humanos. Todas ellas representan foros de análisis, discusión, desarrollo e impulso de políticas y directrices en materia de protección de datos personales direccionadas a partir de la protección

[62] Reglamento de la Red Iberoamericana de Protección De Datos, disponible en *http://www.redipd.es/documentacion/common/REGLAMENTO_RIPD_DIC2018.pdf* , última fecha de consulta el 16 de agosto de 2019.

de los derechos humanos fundamentales que toda persona tiene derecho a proteger.

Como también se puede apreciar en los apartados que anteceden, resulta evidente la existencia del interés y la preocupación por la protección de los datos personales desde diferentes foros internacionales y regionales que proporcionan elementos jurídicos valiosos clave para hacer de la protección de aquellos un derecho cada vez más sólido y consistente capaz de actualizarse y adaptarse a las cada día más apremiantes necesidades de protección jurídica en un mundo en donde el avance tecnológico no se detiene y pone en riesgo la integridad de las personas.

No obstante lo anterior, como bien también se puede apreciar, esos esfuerzos (tanto de la OCDE, como de la OEA y de la RIPDP) resultan ser insuficientes dadas las características propias de esos documentos por ser instrumentos regionales o continentales, faltos de aplicación y vinculación internacional, los cuales, sin embargo, no dejan de ser instrumentos de valiosas aportaciones que merecen y deben ser considerados y apreciados para futuros cuerpos regulatorios con enfoques y alcances más que regionales o sectoriales.

> La generación de estándares comunes con un alcance global acerca de la protección de datos personales no solo es necesaria sino también posible, toda vez que sus cimientos ya han sido establecidos por el propio reconocimiento y desarrollo del derecho a la vida privada. A todo ello se añade el progresivo avance en la materia que se ha venido generando en algunos países del Continente Americano y, aunque con un alcance limitado, en el propio Sistema Interamericano de Derechos Humanos.[63]

[63] Maqueo Ramírez, María Solange, *et. al*., “Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario” [en línea], en *Revista de Derecho Valdivia*, volumen XXX, núm. 1, p. 94, disponible en: *https://scielo.conicyt.cl/pdf/revider/v30n1/art04.pdf*, última fecha de consulta el 17 de agosto de 2019.

Este tipo de esfuerzos esgrimidos y presentados en el presente trabajo desde diferentes foros a escala internacional, son solamente algunos de las diferentes perspectivas que se han considerado con fines a lograr la máxima protección de los datos personales como derecho humano.

Esta tarea se puede considerar como una tarea inacabada e incompleta dados los permanentes y a veces voraces avances de la tecnología, su manifestación y sus consecuentes repercusiones en la sociedad. Tanto es así, que las Naciones Unidas, a través de la Asamblea General, lo ha observado en el documento denominado 'El derecho a la privacidad en la era digital´, en el que establece que:

> …el rápido ritmo del desarrollo tecnológico permite a las personas de todo el mundo utilizar las nuevas tecnologías de la información y las comunicaciones y, al mismo tiempo, incrementa la capacidad de los gobiernos, las empresas y las personas de llevar a cabo actividades de vigilancia, interceptación y recopilación de datos, lo que podría constituir una violación o una transgresión de los derechos humanos, en particular del derecho a la privacidad, establecido en el artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, y que, por lo tanto, esta cuestión suscita cada vez más preocupación.[64]

La anterior manifestación hecha por la asamblea general del máximo organismo tutelador de los derechos humanos a nivel internacional no deja espacio a duda: el cada vez mayor uso y dependencia de las TIC favorecerá paralelamente la creación de cuadros de riesgo a la gama de derechos que le pertenencen y le son propios a las personas, en este caso, el derecho a la privacidad.

---

[64] Organización de las Naciones Unidas, Asamblea General, "El derecho a la privacidad en la era digital", 31 de octubre de 2016, disponible en: *https://www.acnur.org/fileadmin/Documentos/BDL/2017/10904.pdf*, última fecha de consulta el 22 de octubre de 2019.

Con ello, se puede hacer evidente constancia de que existen diversos organismos e instituciones con alcances globales o regionales comisionados o encargados de salvaguardar y proteger los derechos humanos, mismos que emiten documentos que a manera de estándares o principios hacen un llamado para que los países pertenencientes a sus foros, tracen, desarrollen y apliquen esquemas y modelos de protección a los datos personales.

2.2.4 La Corte Interamericana de Derechos Humanos y el derecho a la protección de datos personales

Finalmente, se presenta una breve descripción de lo que hasta el momento ha sucedido en cuanto a la CIDH en relación al derecho a la protección de datos personales, esto por lo que hace al Sistema Interamericano de Derechos Humanos por ser México un país miembro de este subsistema y al cual se ve obligado cumplir y observar por cuanto a las resoluciones y sentencias que se lleguen a dictar en contra de México, esto conforme se estipula en el artículo 68 de la Convención Americana sobre Derechos Humanos, que a la letra establece que "Los Estados Partes en la Convención se comprometen a cumplir la decisión de la Corte en todo caso en que sean partes",[65] prescripción que además, fue fortalecida por nuestra Suprema Corte de Justicia al darle resolución a la contradicción de tesis número 293/2011, en relación con el valor de la jurisprudencia de la CIDH, al establecerse que "en cuanto al segundo tema relativo al valor de la jurisprudencia emitida por la Corte IDH, el Tribunal Pleno determinó por mayoría de 6 votos, que *la jurisprudencia emitida por la Corte Interamericana*

[65] Convención Americana sobre Derechos Humanos, disponible en *https://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.htm*, última fecha de consulta el16 de agosto de 2019.

de Derechos Humanos es vinculante para los todos los órganos jurisdiccionales, siempre que dicho precedente favorezca en mayor medida a las personas".[66]

En ese sentido, se considera valioso hacer notar que a pesar de que el derecho a la protección de datos personales se encuentra incorporado e instituido en las constituciones de muchos países, no solo del continente americano sino de muchos países a escala internacional, tal derecho puede llegar a ser considerado, inclusive, solamente desde un carácter instrumental para dotar de efectividad el derecho a la privacidad.

> "De hecho, es valioso observar que hasta el momento la Corte Interamericana de Derechos Humanos (en adelante, CIDH) no se ha pronunciado de manera específica en ningún caso respecto del derecho a la protección de datos personales, a pesar de que un gran número de países sujetos a su jurisdicción lo contemplan dentro de su propio derecho interno con el carácter de derecho humano. De tal forma que, como veremos, el desarrollo internacional de la protección de datos personales se produce a nivel regional y, fundamentalmente en Europa, a partir de la propia construcción expansiva del derecho a la vida privada hasta el reconocimiento de su propia autonomía".[67]

Con esto se puede llegar a la conclusión de este apartado, de que el derecho a la protección de datos, aun siendo considerado como un derecho

---

[66] Suprema Corte de Justicia de la Nación, Contradicción de Tesis 293/2011, disponible en: *http://www2.scjn.gob.mx/asuntosrelevantes/pagina/seguimientoasuntosrelevantespub.aspx?id=129659&seguimientoid=556*, última fecha de consulta el 29 de agosto de 2019. [El subrayado es de origen].

[67] Maqueo Rmírez, María Solange, *et. al.*, Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario, Revista de derecho, vol. XXX, No. 1, junio de 2017, disponible en: https://scielo.conicyt.cl/pdf/revider/v30n1/art04.pdf, consultado el: 29 de agosto de 2019.

humano autónomo al derecho a la privacidad, conforme se encuentra instituido en muchas constituciones, sigue siendo, hasta el momento, considerado como parte instrumental y adhesivo a un derecho humano de implicaciones y repercusiones más amplias y de mayor calado como lo es el derecho a la privacidad, lo cual, de acuerdo a lo ofrecido previamente, también es así entendido y practicado por la CIDH.

2.3 Contexto nacional del derecho a la protección de datos personales

Actualmente en México, al igual que muchos países (ver tabla 1, capítulo 1), el derecho a la protección de datos personales ha tomado mayúscula relevancia e importancia al grado de ser expresamente recogido en nuestra Carta Magna, siendo específicamente el artículo 6, párrafo segundo, en el cual se instituye que:

> Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, 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.

Esta expresa mención constitucional sobre el derecho a la protección de datos personales, sin embargo, debió de haber recorrido un largo camino legislativo colmado de propuestas y planteamientos relativos a la protección de los datos personales sin que se obtuviera en concreto algún resultado satisfactorio y pertinente en la materia. “En México, desde el año 2000, se han promovido diversos proyectos legislativos en torno a la protección de datos personales en el Congreso de la Unión, sin que ninguno de ellos fructificara, dada la ausencia de una disposición constitucional que les diera sustento”.[68]

[68] Presentación al libro “Presentación al libro “Protección de datos personales. Compendio de lecturas y legislación”, *op. cit*., nota 53.

No siendo propósito fundamental del presente trabajo hacer una relatoría sobre el largo camino que debió de haber recorrido la inclusión en la constitución mexicana del derecho a la protección de datos personales, se considera suficiente hacer el señalamiento de que a ya más de una década, este derecho, materia del presente trabajo, se encuentra expresamente establecido en nuestra constitución y que tal procedimiento debió de haber sido la expresión de un ejercicio legislativo con miras de dotar a la ciudadanía mexicana de herramientas y mecanismos jurídicos asibles y prontos para la protección de sus derechos, por lo que:

> Después de un proceso democrático sin precedentes, en el que la Cámara de Diputados el 06 de marzo aprueba por unanimidad (1 abstención, 425 votos en total) y la Cámara de Senadores aprueba también por unanimidad el 24 de abril (111 votos, 0 abstenciones) y lo ratifican congresos de diferentes Estados de la República; 12 finalmente el texto de la reforma al artículo 6 constitucional finalmente se publica el 20 de julio de 2007 en los siguientes términos[69]:
>
> Artículo 6º de la Constitución Mexicana
>
> (…)
>
> 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:
>
> (…)
>
> 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.

[69] Puente de la Mora, Ximena, “Reforma al artículo 6 constitucional que considera el acceso a la información como derecho fundamental en México, retos y perspectivas” *Revista de Derecho Informático*, núm. 139, 2010, p. 5, disponible en: *http://www.alfa-redi.org/sites/default/files/articles/files/puente_2.pdf*, última fecha de consulta el 25 de agosto de 2019.

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.

(…)

Se puede establecer que esta reforma, como previamente se señaló, tuvo origen y propósito el establecer el andamiaje constitucional sobre el cual se estableciera toda la subsecuente estructura jurídica regulatoria del derecho de acceder a la información que ostentase cualquier autoridad pública, pues a partir de esta reforma, "se pudieron crear los procedimientos y las instituciones para permitir que, a nivel federal, cualquier persona pudiera, mediante la presentación de una solicitud de acceso a la información, obtener acceso a los documentos gubernamentales".[70]

También se puede establecer que uno los principales resultados de las reformas previamente referidas, fue la creación y posterior reconfiguración del entonces IFAI , instituyéndose desde ese momento como la instancia responsable de garantizar el ejercicio del derecho al acceso a la información pública que entonces se encontraba en ciernes. Así, "La historia del IFAI, su naturaleza jurídica, atribuciones y diseño institucional, están inexorablemente ligados a las circunstancias que rodearon la creación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental en México".[71]

Sin embargo, las facultades y potestades del IFAI fueron poco a poco extendiéndose, originándose de esa manera la necesidad de incluir dentro del marco de actuación de tal Instituto la protección de igual manera del derecho a la protección de datos personales, siendo que "…con el paso del tiempo y la especialización que fue dándose al interior de la Institución, la faceta de autoridad

[70] Caballero, José Antonio, *et. al.*, "El futuro del Instituto Federal de Acceso a la Información Pública y Protección de Datos Personales: consideraciones sobre su autonomía constitucional", *Revista electrónica*, núm. 7, 2012, p. 3, disponible en *https://archivos.juridicas.unam.mx/www/bjv/libros/7/3196/1.pdf*, última fecha de consulta el 28 de agosto de 2019.

[71] *Idem*, p. 5.

garante de la protección de los datos personales contenidos en los ficheros públicos (…) comenzó a desarrollarse, si bien, el ejercicio de los derechos de acceso y rectificación de datos fue plenamente observado desde el inicio por los entes gubernativos".[72]

Posteriormente, como derivado de la reforma constitucional de 2014 y con la emisión de la Ley General de Transparencia y Acceso a la Información Pública, el entonces IFAI cambia su nombre por el del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, destacándose de la reforma, entre otras cosas:

> Que el órgano garante constitucional del derecho a la protección de datos personales presenta un desdoblamiento de funciones: (1) Por una parte es el órgano 'federal', cuyo ámbito de competencia se extiende a los sujetos obligados de carácter federal y, en su caso, a los responsables de datos personales del sector privado de conformidad con la LFPDPPP (esto es, en el supuesto de que no se cree una nueva entidad encargada de la protección de datos personales en posesión de los particulares), y (2) Por otra parte se constituye en un verdadero órgano de carácter 'nacional', cuyas potestades están dirigidas a garantizar la efectividad del derecho humano a la protección de datos personales, toda vez que tiene la capacidad de intervenir tanto en el orden jurídico federal como estatal.[73]

---

[72] Peschard Mariscal, Jaqueline, "El Instituto Federal de Acceso a la Información Pública como órgano garante en materia de Protección de Datos Personales", en *Protección de datos personales. Compendio de lecturas y legislación*, México, Tiro Corto Editores, 2010, p. 113.

[73] Maqueo Ramírez, María Solange y Moreno, Jimena, "Implicaciones de una ley general en materia de protección de datos personales", en *Revista especializada del Centro de Investigación y Docencia Económica* (CIDE), núm. 64, p. 13, disponible en: *https://docplayer.es/19273602-Maria-solange-maqueo-y-jimena-moreno.html*, última fecha de consulta el 28 de agosto de 2019.

Finalmente, y con acuerdo a lo instituido en su página oficial, el INAI es un organismo constitucional autónomo garante del cumplimiento de dos derechos fundamentales: el de acceso a la información pública y el de protección de datos personales, siendo en ese sentido que:

- Para el primero, garantiza que cualquier autoridad en el ámbito federal, órganos autónomos, partidos políticos, fideicomisos, fondos públicos y sindicato; o cualquier persona física, moral que reciba y ejerza recursos públicos o realice actos de autoridad te entregue la información pública que solicites.
- Para el segundo, garantiza el uso adecuado de los datos personales, así como el ejercicio y tutela de los derechos de acceso, rectificación, cancelación y oposición que toda persona tiene con respecto a su información".[74]

Con lo hasta aquí expuesto, se puede entender en términos muy amplios cómo es que ha sido la inclusión del derecho a la protección de datos personales en la carta magna mexicana, teniendo como característica fundacional la relación intrínseca entre los derechos de acceso a la información pública y el de protección de datos personales, siendo este último derecho el que, después de un considerable trabajo legislativo y consecuentes proyectos de reforma a diferentes artículos constitucionales concernientes a la materia, fue que se dio espacio a la institucionalización constitucional del derecho a la protección de datos personales en México.

2.3.1 Relación entre los derechos de acceso a la información pública y el de protección de datos personales en México

La expresa inclusión al derecho a la protección de datos personales en el cuerpo normativo constitucional de nuestra nación no fue concebido y desarrollado desde una perspectiva única y exclusiva como un derecho autónomo e independiente, sino que debió de tener sus orígenes derivado del desarrollo normativo de otro

[74] Página oficial del INAI, disponible en: *http://inicio.inai.org.mx/SitePages/que-es-el-inai.aspx*, última fecha de consulta el 28 de agosto de 2019.

derecho “nuevo” en el sistema jurídico mexicano, el derecho de acceso a la información pública. “Con esta acción se abrió la puerta al reconocimiento de otro derecho: el de protección de los datos personales. Al proteger la información confidencial en las legislaciones de transparencia que, desde el 2002, fueron creadas, se protegieron los datos personales ante posibles intromisiones de los solicitantes”.[75] Así:

“en el 2002 se aprueba por unanimidad en el Congreso esta Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (…), que incluye como objetivos primordiales transparentar la gestión pública mediante la difusión de la información y favorecer la rendición de cuentas, (…) y también *garantizar la protección de los datos personales* en posesión de los sujetos obligados para “contribuir a la democratización de la sociedad mexicana y a la plena vigencia del Estado de Derecho.[76]

Con esto podemos darnos cuenta de cómo han sido los orígenes del derecho a la protección de datos personales, el cual, como previamente se ha referido, tiene sus orígenes en el desarrollo del derecho de acceso a la información pública, siendo que, en ejercicio de este derecho, se ponía en riesgo los derechos de las personas sobre las cuáles se llegara a solicitar información pública pudiendo entregarse información personal concerniente a los funcionarios públicos que los pudiera comprometer o poner en riesgo al revelarse su propia información personal, por lo que, “[e]n esa ley, la protección de datos personales

[75] Guerra Ford, Oscar M., “Las legislaciones de protección de datos personales en el país”, en *Retos de la protección de datos personales en el sector público* [en línea], México, Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, México, 2011, p. 107, disponible en: *http://www.infodf.org.mx/comsoc/campana/2012/LIbrodatosPweb.pdf*, última fecha de consulta el 19 de agosto de 2019.

[76] Puente de la Mora, Ximena, *op. cit.*, nota 73, p. 5.

todavía era insoslayable y dependiente del derecho de acceso a la información y no contaba con el carácter de un derecho autónomo".[77]

Así entonces, "[e]l mencionado artículo 6, fracción II, tiene la virtud de ser la primera disposición en la historia de nuestro país que hace un reconocimiento expreso al derecho a la protección de datos personales en la cúspide normativa, dando continuidad a la labor iniciada por el legislador ordinario a través de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental".[78]

2.3.2 La Ley General de Transparencia y Acceso la Información Pública y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

Como se ha venido señalando en los párrafos que anteceden, el origen de los derechos de acceso a la información pública y el de protección de datos personales presentan patentemente una característica singular entre ambos, puesto que como ha sido manifestado en apartados previos, el segundo de los derechos puede llegar a considerarse como una especie de limitante y/o derivación del primero.

Esta particularidad entre ambas normatividades aún se puede ejemplificar manifiesta y expresamente, puesto que en la actual y vigente Ley general se encuentra instituido el mandato que establece que cada *responsable* obligado ante la misma ley, "contará con un Comité de Transparencia, *el cual se integrará y funcionará conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública* y demás normativa aplicable*",* siendo tal comité, "la

---

[77] Iniciativa con proyecto de decreto por la que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, *op. cit*., nota 44, p. 3.

[78] Ornelas Núñez, Lina y López Ayllón, Sergio, "La recepción del derecho a la protección de datos en México: breve descripción de su origen y estatus legislativo", en *Protección de datos personales. Compendio de lecturas y legislación*, México, Tiro Corto Editores, 2010, p. 66.

autoridad máxima en materia de protección de datos personales dentro de cada responsable, teniendo, entre otras funciones: I. Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con las disposiciones previstas en la presente Ley y en aquellas disposiciones que resulten aplicables en la materia". [79]

Más adelante, en el artículo 85 de la misma ley, se establece que cada responsable contará, además, con una Unidad de Transparencia, la cual, una vez más, se integrará y funcionará conforme a la misma *Ley General de Transparencia y Acceso a la Información Pública*, estableciéndose que dentro de sus funciones tendrá, entre otras cosas, que: 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.

Con lo hasta aquí expuesto, no puede quedar espacio a duda sobre la evidente interdependencia existente entre ambos cuerpos normativos en la protección y defensa de sus correspondientes derechos. Este punto retoma importancia con relación a la protección de datos personales dentro de los sujetos responsables conforme la normatividad general lo establece, puesto que la Universidad Politécnica de Texcoco, objeto de este trabajo, se configura como sujeto responsable en la protección de los datos personales de los cuales hacen tratamiento y que por tal situación se encuentra obligada a observar y a acatar la normativa aplicable en la materia.

Todo lo anterior con miras a prevenir y, en determinado momento, actuar en todo momento con acuerdo a lo establecido en los instrumentos tanto internacionales y regionales en materia de protección de datos lo cual, lo que, a final de cuentas, tendrá con fin último la máxima protección posible a los derechos inherentes de las personas y en este caso en concreto, el derecho del alumnado a

---

[79] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, artículo 83, últma fecha de consulta el 29 de agosto de 2019. [Las cursivas son propias].

saber a quién ha confiado su información personal y que tratamiento es el que se le da y con base a qué normatividad.

2.4 Contexto local de la protección de datos personales en el Estado de México

Ahora bien, como ya previa y reiteradamente se ha manifestado, el objeto del presente trabajo lo es UPTex, institución educativa que, con acuerdo a su decreto de creación, se configura como un organismo público descentralizado de la administración pública del estado de México, sectorizada a la Secretaría de Educación estatal.[80]

Este último hecho, el de pertenecer a la dependencia estatal encargada de planear, organizar, dirigir y evaluar la prestación de servicios educativos en el Estado de México, hace a la UPTex ubicarse dentro del catálogo de sujetos obligados a la protección de datos personales conforme lo establece la normatividad estatal y general aplicable a la materia, tal y como se puede constatar en la página oficial del Instituto de Transparencia, Acceso a la información Pública y Protección de Datos Personales en el Estado de México y Municipios (en adelante Infoem),[81] órgano garante del derecho a la protección de datos personales en el estado.

Descrito el anterior contexto, a continuación, se presenta el marco normativo en materia de protección de datos personales aplicable y vigente en el Estado de México y sus municipios, y a partir del cual se vierten las disposiciones

---

[80] Decreto del Ejecutivo del Estado de México por el que se crea el Organismo Público Descentralizado de carácter estatal denominado Universidad Politécnica de Texcoco, disponible en: *http://uptexcoco.edomex.gob.mx/sites/uptexcoco.edomex.gob.mx/files/files/Acta_Decreto%20de%20creaci%C3%B3n%20UPTex.pdf*, última fehca de consulta el 30 de agosto de 2019.

[81] Sitio oficial del Infoem, disponible en: *http://www.infoem.org.mx/src/htm/poderEjecutivo.html*, última fecha de consulta el 30 de agosto de 2019.

y directrices que organismos como la UPTex, como sujeto obligado, se encuentra constreñida a observar y acatar.

2.4.1 Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios

Para hacer introducción al siguiente apartado, se considera oportuno hacer una corta pero muy importante mención en relación al actual sistema competencial establecido en México, puesto que de acuerdo a lo instituido en el artículo 40 constitucional, “Es voluntad del pueblo mexicano constituirse en una República representativa, democrática, laica y federal, compuesta por *Estados libres y soberanos en todo lo concerniente a su régimen interior*, y por la Ciudad de México, unidos en una federación establecida según los principios de esta ley fundamental”.

Así pues, conforme lo instituye el numeral constitucional previamente referido, se comprenden a todas las entidades federativas componentes de la república mexicana como partes integrantes de un solo ente soberano estando todos y cada uno de ellos constreñidos y unidos por el pacto federal de gobernabilidad, pero que no obstante ello, pueden y deben, dentro de lo reconocido y facultado, hacer ejercicio de la soberanía que en ellos se deposita para de esta forma legislar en los diferentes ámbitos y materias que le conciernen.

Acotado lo anterior, y en plena semejanza a lo sucedido en el panorama nacional, los legisladores del congreso mexiquense percibieron la necesidad de reformar la constitución local en materia de transparencia por parte del constituyente local con el fin de cumplir con los estándares previstos en la reforma al artículo sexto constitucional nacional, por lo que derivado de las reformas al artículo 5o. de la Constitución Política del Estado Libre y Soberano de México, en el párrafo décimo primero se reconoce el derecho a la protección de datos personales, al establecer lo siguiente: “Los Poderes Públicos y los organismos autónomos transparentarán sus acciones, garantizarán el acceso a la información pública *y protegerán los datos personales* en los términos que señale la ley

reglamentaria",[82] reforma a la constitución local que cimienta las bases para la protección y corrección de datos personales.

Así los previos antecedentes, en el Estado de México, en ejercicio de la soberanía que ostenta hacia su régimen interior, es que en fecha 30 de mayo de 2017 se publica en la Gaceta del Gobierno del Estado Libre y Soberano de México la actual y vigente Ley local de protección de datos. "De este modo, el Estado de México se convirtió en la segunda entidad federativa en realizar la armonización con la norma nacional, dos meses antes del término fijado por el legislador federal".[83]

Misma ley que además de adecuarse a los parámetros establecidos en la Ley general de la materia,

> …se adicionaron o adecuaron figuras que se consideraron necesarias de acuerdo con la experiencia local en la materia, como el Programa Estatal de Protección de Datos Personales; la protección de datos personales de menores y datos personales sensibles; la clasificación de datos personales a través de acuerdos relativos a sus sistemas; la definición de deberes a cargo de los responsables, su

---

[82] Exposición de motivos de la Ley de Protección de Datos Personales del Estado de México, disponible en: *https://seduc.edomex.gob.mx/sites/seduc.edomex.gob.mx/files/files/acerca/Marco%20Juridico/Ley%20de%20Protecci%C3%B3n%20de%20Datos%20Personales%20del%20Estado%20de%20M%C3%A9xico.pdf*, última fecha de consulta el 3 de septiembre de 2019.

[83] Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios, julio de 2017, p 12, disponible en: *https://www.infoem.org.mx/doc/publicaciones/LeyDeDatosPersonales.pdf*, última fecha de consutla el 1 de septiembre de 2019.

> conceptualización e integración con disciplinas como la administración documental y el gobierno digital; la incorporación del concepto de administrador; el reconocimiento de nivel adecuado de protección; la participación en la Plataforma Nacional a través del Sarcoem; el Centro de Atención Telefónica; *la obligatoriedad del oficial de Protección de Datos Personales y el responsable en Materia de Seguridad para tratamientos relevantes o intensivos*; la cláusula en el testamento para ejercicio de derechos ARCO, y la limitación del tratamiento, entre otras.[84]

De esta forma y como se puede apreciar, se puede considerar que el legislador mexiquense emite un cuerpo normativo adaptado y actualizado a las ahora existentes demandas y exigencias en materia de protección de datos personales poniendo, como ejemplos, énfasis en la protección de datos personales en menores, aspecto que requiere de la máxima atención y diligencia dado el grado de importancia que implica tal materia.

Por otra parte, en el mismo cuerpo normativo, se hace también señalamiento expreso sobre la obligatoriedad de designar a *oficial de Protección de Datos Personales y el responsable en Materia de Seguridad para tratamientos relevantes o intensivos en cada sujeto obligado*, disposición que para efectos del presente trabajo retoma especial relevancia dado que serán estas figuras los que en determinado momento sean las que se encarguen de administrar y gestionar los SGDP, sistema como el que en el presente trabajo se propone.

Adentrándonos un poco en la Ley local, y con acuerdo a lo estipulado en el párrafo segundo del artículo 1, este estatuto “Tiene por objeto establecer las bases, principios y procedimientos para tutelar y garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de los sujetos

---

[84] Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios, *op. cit*., nota 88, [Las cursivas son propias].

obligados”[85], misma ley que en el numeral tercero se enlistan los sujetos obligados a observar dicho cuerpo legal, siendo los siguientes:

> Artículo 3. Son sujetos obligados por esta Ley:
> I. El Poder Ejecutivo.
> II. El Poder Legislativo.
> III. El Poder Judicial.
> IV. Los Ayuntamientos.
> V. Los Órganos y Organismos Constitucionales Autónomos.
> VI. Los Tribunales Administrativos.
> VII. Los Partidos Políticos.
> VIII. Los Fideicomisos y Fondos Públicos.

Como previamente ya se había referido, en el caso de la UPTex objeto del presente trabajo, por ser sectorizada a la Secretaría de Educación mexiquense, se ubica dentro de la estructura del Poder Ejecutivo estatal y, por lo tanto, se reitera, se configura como institución obligada a observar las disposiciones en materia de protección de protección de datos personales.

Así pues y no obstante esta potestad soberana de cada estado de legislar en los asuntos locales concernientes a las diferentes materias que le competen y corresponden y a las que constitucionalmente están obligados a actuar, se precisó necesaria la creación de un cuerpo normativo generalizado y aplicable a toda la nación en materia de protección de datos personales en el sector público.

En ese sentido, una vez más se tuvo que echar a andar la maquinaria legislativa federal con el objetivo de establecer el andamiaje normativo en materia de protección de datos personales en el sector público con miras a obtener un

---

[85] Decreto número 209 por el que se expide la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, disponible en: *https://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/pdf/gct/2017/may305.pdf*, última fecha de consulta el 31 de octubre de 2019.

instrumento jurídico suficiente y bastante que se implantase en todos los estados de la república y órdenes de gobierno (federal, local y municipal), inquietud que fue considerada y recogida en la exposición de motivos de la Ley local de protección de datos al señalarse que:

> Estas modificaciones constitucionales poseen un matiz histórico en materia de datos personales, pues, (…) 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.[86]

Siendo así, como resultado de este ejercicio legislativo es que en fecha 26 de enero de 2017 se publica la última reforma *en materia de transparencia* emitiéndose en el Diario Oficial de la Federación la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados con lo que, "En consecuencia, esta Ley General marca un hito importante en la protección de datos personales en posesión de entes públicos, puesto que establece los principios, bases y procedimientos que deben regir en los tres niveles de gobierno en México".[87]

De esta forma, y como se hizo disposición expresa en el artículo 2 transitorio de la nueva ley general, se mandató a todas las legislaturas locales a

---

[86] Iniciativa con proyecto de decreto por la que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, *op. cit*., nota 44, p. 5. [El subrayado es propio].

[87] Sánchez Hernández, Luis Ricardo, "Sistematización de obligaciones en materia de protección de datos personales para el sector público en el Estado de México", *Tesis de maestría en Derecho de las Tecnologías de la Información y Comunicación*, Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación (INFOTEC), Ciudad de México, 2017, p. 46, disponible en: *https://infotec.repositorioinstitucional.mx/jspui/handle/1027/2*, última fecha de consulta el 1 de septiembre de 2019.

“ajustarse a las disposiciones previstas en esta norma en un plazo de seis meses siguientes contado a partir de la entrada en vigor de la presente Ley”, contexto que demuestra cómo es que ambas ejercicios soberanos tanto de orden estatal o local como federal, se ensamblan para tratar de establecer un marco normativo concurrente acorde a las necesidades e inquietudes por proteger y salvaguardar los datos personales de los ciudadanos en posesión de los entes, organismos y dependencias del sector público, siendo en este caso, del gobierno del estado de México.

> Así, a través de este instrumento legal, se distribuyen competencias entre los Organismos garantes de la Federación y las Entidades Federativas, en materia de protección de datos personales en posesión de sujetos obligados; se establecen las bases mínimas y condiciones homogéneas que regirán el tratamiento de los datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, mediante procedimientos sencillos y expeditos; así como garantizar la observancia de las disposiciones previstas en Ley de manera uniforme en todo el país”.[88]

Con la entrada en vigor de la ley general es que se creen cimientos más firmes y concretos en la regulación del derecho a la protección de datos personales en todo México, esto por tratarse del marco jurídico general aplicable de manera directa a la federación y a partir del cual las etidades federativas han de diseñar y adoptar su propio régimen legal y poder con ello emitir las diversas medidas regulatorias en los distíntos órdenes de gobierno.

[88] Sánchez Hernández, Luis Ricardo, *op. cit.*, nota 92, p. 46.

2.4.2 Normatividad complementaria a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios

Finalmente, a continuación, se presentan brevemente tres cuerpos normativos relativos y complementarios a la Ley local de protección de datos para su aplicación conjunta en la materia.

Así pues, en primer lugar se mencionará los "Lineamientos por los que se establecen las políticas, criterios y procedimientos que deberán observar los sujetos obligados, para proveer la aplicación e implementación de la Ley de Protección de Datos Personales del Estado de México" (en adelante los Lineamientos), pero antes de ello, se aprecia indispensable hacer el señalamiento de que tales lineamientos, hasta la fecha no han sido objeto de actualización, pero que no obstante ello, los mismos pueden ser utilizados a forma de referencia, siempre y cuando no se contrapongan a alguna disposición expresa ya sea de la Ley General en la materia o de la Ley local de protección de datos.

> Así entonces, tales lineamientos, con acuerdo a lo estipulado en el artículo 1, "…son de observancia obligatoria para los Sujetos Obligados y tienen por objeto establecer las políticas, criterios y procedimientos para proveer la aplicación e implementación de la Ley de Protección de Datos Personales del Estado de México".[89]

En segundo lugar, y con acuerdo al artículo 14 de la Ley local de protección de datos, se responsabiliza al Infoem para diseñar, ejecutar y evaluar un programa estatal de protección de datos personales, a partir del cual habrá de definirse la

[89] Lineamientos por los que se establecen las políticas, criterios y procedimientos que deberán observar los Sujetos Obligados, para proveer la aplicación e implementación de la Ley de Protección de Datos Personales del Estado de México, disponibles en: *https://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/vigentes/may031.PDF*, última fecha de consulta el 3 de septiembre de 2019.

política pública estatal en materia de protección de datos personales en el Estado de México, estableciendo objetivos, estrategias, acciones y metas, conforme a las siguientes bases:

> I. Hacer del conocimiento general el derecho a la protección de datos personales; II. Promover la educación y una cultura de protección de datos personales entre la sociedad mexiquense; III. Fomentar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición; IV. Capacitar a los sujetos obligados en materia de protección de datos personales; V. Certificar a los sujetos obligados, organizaciones o asociaciones de la sociedad, así como personas en general, que ofrezcan, en forma interdisciplinaria y profesional, la posibilidad de llevar a cabo cursos o talleres en materia de protección de datos personales; VI. Impulsar la implementación y mantenimiento de un sistema de gestión de seguridad a que se hace referencia en la presente Ley, así como promover la adopción de estándares nacionales e internacionales y buenas prácticas en la materia, y VII. Prever los mecanismos que permitan medir, reportar y verificar las metas establecidas.[90]

Finalmente, existe dentro de la normatividad estatal en materia de protección de datos personales en posesión de sujetos obligados un tercer cuerpo regulatorio, en esta ocasión emitido por el Infoem en ejercicio de su facultades y obligaciones como órgano garante estatal, enfocado en este caso concretamente, a las medidas de seguridad aplicables a los Sistemas de Datos Personales, denominado “Lineamientos sobre medidas de seguridad aplicables a los sistemas

[90] Programa Estatal de Protección de Datos Personales del Estado de México, disponible en: *http://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/pdf/gct/2018/may317.pdf*, última fecha de consulta el 3 de septiembre de 2019.

de datos personales que se encuentran en posesión de los sujetos obligados de la ley de protección de datos personales del Estado de México".

Este tópico se considera cardinal para los propósitos y consecución del principal objetivo del presente proyecto, puesto que lo que se pretende obtener es el diseño de un SGDP para la UPTex, mismo que tendrá que ser diseñado conforme a los parámetros y directrices establecidos en la regulación y normatividad aplicable a la materia como los lineamientos que previamente se señalaron.

Preciso es hacer el señalamiento de que, al igual que los Lineamientos, este cuerpo técnico regulatorio aún no ha sido actualizado y no obstante esa situación, se consideran aprovechables, siempre y cuando no se contrapongan a alguna disposición expresa ya sea de la Ley General en la materia o de la Ley local de protección de datos.

Así precisado lo anterior, en las consideraciones vertidas sobre este cuerpo regulatorio, se establece que tales disposiciones "buscan dar certeza sobre las tareas u obligaciones que los Sujetos Obligados deben observar en materia de medidas de seguridad aplicables a los sistemas de datos personales en su poder, tanto físicos como automatizados", ya que lo que se busca alcanzar con estos lineamientos es "ser un instrumento de disposiciones específicas para lograr la mayor protección de los datos personales, para que los Sujetos Obligados puedan lograr un estándar de seguridad al respecto, sin perjuicio de que éstos establezcan medidas adicionales que coadyuven a la mejor protección de los datos personales".[91]

[91] 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, disponible en: *https://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/vigentes/may083.PDF*, última fecha de consulta el 4 de septiembre de 2019.

2.5 Consideraciones finales al capitulo dos

Como se puede observar, con el afán de ir a la par a lo acontecido y exigido en el escenario nacional con la emisión de la ley general en la materia, los legisladores del congreso estatal mexiquense por una parte y el Infoem por otra, han establecido y fijado cuerpos normativos, políticas y directrices en materia de la protección de datos personales en el ámbito estatal con miras a alcanzar la máxima protección de este derecho que como se ha referido en previas ocasiones, se pone cada vez más en riesgo como consecuencia del desarrollo y práctica de las nuevas tecnologías que tienen como esquema fundacional la utilización de información personal.

Así pues, el marco jurídico descrito previamente en materia de protección de datos personales en el estado de México habrá de ser la estructura legal y reglamentaria sobre la cual se diseñe el SGDP para la UPTex, institución educativa obligada a observar tal cuerpo normativo.

Capítulo 3

Propuesta de intervención: diseño de un sistema de gestión de datos personales para la Universidad Politécnica de Texcoco

Capítulo 3. Propuesta de intervención: diseño de un sistema de gestión de datos personales para la Universidad Politécnica de Texcoco

Como se puede apreciar en el capítulo que antecede, la preocupación por la protección de los datos personales es un fenómeno social con claras y evidentes incidencias en el actual mundo jurídico. Esta situación, como también se pudo constatar, ha sido abordada y tratada por organizaciones internacionales y multilaterales que, dentro de sus respectivos foros, se han dado a la tarea de elaborar y emitir diversos documentos que con el carácter de directrices, principios y estándares han manifestado de alguna u otra manera esta preocupación y como resultado de ello, sobre todo, se han establecido y aportado muy valiosos elementos y particularidades a partir de los cuales el derecho a la protección de datos personales ha de encauzarse con el fin último de lograr la máxima protección de la información personal.

En ese contexto, y previo descrito el marco jurídico normativo tanto de orden nacional como local a través del cual el presente trabajo habrá de estructurarse y diseñarse, en el presente capítulo se ofrecerá la descripción procedimental general con base a la cual se diseñará el SGDP para la UPTex, institución educativa que como previamente ha quedado determinado, se configura como sujeto obligado a observar la normatividad en la materia y que por lo tanto se encuentra constreñida a adoptar e implementar referido sistema.

Así pues, la posibilidad de que tal institución cuente con un SGDP adaptado sustancialmente a sus propias y definidas características podrá permitir que la universidad colme las prescripciones exigidas en la normatividad en materia de protección de datos personales tanto de la Ley General como de la Ley local de protección de datos y con ello no situarse como potencial objetivo de responsabilidades y sanciones derivadas de la inobservancia como así lo instituye la normatividad en la materia.

En ese sentido, resulta preciso hacer hincapié sobre la obligación que instituciones educativas como la UPTex asumen al configurarse como un organismo público descentralizado de la administración pública del Estado de México, sectorizado a la Secretaría de Educación estatal, situación que hace que se coloque dentro del listado de sujetos obligados a cumplir los cuerpos jurídicos en la materia.

Esta particularidad se puede considerar de especial importancia para las instituciones educativas como en este caso la UPTex, puesto que al contar con esquemas y procedimientos sistematizados de control y gestión de la información personal que ostentan tanto del alumnado como del cuerpo docente y personal administrativo, permitirá que tal universidad, como se refirió previamente, satisfaga lo establecido en la normatividad en la materia, pero principal y máximamente, podrá ofrecer la seguridad de que tal información es tratada de acuerdo a los actuales estándares de seguridad y protección de datos personales y con ello pueda seguir contando con el crédito y la aprobación por parte de la población estudiantil que se encuentra adscrita o pretenda enrolarse en alguno de los planes de estudios que tal institución ofrece.

Acotado lo anterior, se establece que la meta principal del presente trabajo es diseñar en términos generales un SGDP para la UPTex, mismo que tendrá que ser estructurado con acuerdo a las características y naturaleza propias de la Universidad, mismas que incidirán directamente en el diseño del SGDP, puesto que factores propios de la institución, como por ejemplo la matrícula de alumnos y el tipo de datos personales que la universidad recaba y a los cuales da tratamiento, determinarán sustancialmente el diseño de tal sistema.

En ese sentido, también es preciso hacer el señalamiento de que el SGDP que aquí se propone diseñar, pretende establecer únicamente la estructura y el esquema generales con base a las cuales el SGDP habrá de desarrollarse, puesto que la implementación y la operación de este, dados los alcances e importancia que conllevan, habrán de gestionarse y aplicarse en una etapa posterior dentro de la institución.

Finalmente, es preciso hacer el señalamiento de que el diseño del SGDP para la UPTex que aquí se propone, se desarrollará substancialmente con base en lo establecido en la Ley local de protección de datos y sus respectivos Lineamientos a los que se han hecho referencia en el capítulo que antecede, además de apegarse a lo establecido en los diversos estándares que proporcionan un marco de gestión de la información personal utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

Resulta en ese sentido válido señalar que, si bien en la actualidad existe una diversidad de marcos de referencia para la gestión de la información personal, el ISO 27001 continúa siendo un estándar utilizado internacionalmente con este propósito, situación que es considerada y replicada en México. Es por ello por lo que ha sido utilizado como un punto de partida para establecer y diseñar el SGDP y, aunque en la actualidad no se menciona de forma explícita un modelo de mejora continua, el ciclo de Deming sigue siendo una referencia.

3.1 La Universidad Politécnica de Texcoco como sujeto responsable y el estado actual en materia de protección de datos personales

La UPTex es una institución educativa de relativa reciente creación. Sus orígenes se remontan al 2011, año en el que se publica en la Gaceta de Gobierno del Estado de México su decreto de creación, instrumento que sustenta y respalda la vida jurídica e institucional de dicha universidad.

Esta situación pone de manifiesto que la aludida institución, como naturalmente habrá de entenderse, aún carezca de determinados esquemas y mecanismos de carácter técnico administrativo que le permitan, por una parte, llevar a cabo las tareas y actividades de carácter administrativas y de control de la información de manera óptima, e impide consecuentemente, por otra parte, cumplir con las disposiciones jurídicas relativas y aplicables a las actividades y funciones propias de dicha institución, como lo es en este caso, la normatividad en materia de protección de datos personales.

Así pues y no obstante el hecho de ser una institución de reciente creación y de contar con una matrícula de alumnos y personal docente y administrativo relativamente baja,[92] la Universidad no se libera ni se exime de acatar y observar las disposiciones establecidas en materia de protección de datos personales tanto de carácter general como local.

Es precisamente esta situación, la de ser una universidad pública de dimensiones y estructuras relativamente pequeñas las que dan motivo y razón al propósito de llevar a cabo el presente trabajo, ya que, al ser una institución de referidas proporciones, podrá permitir que el SGDP que aquí se diseñe pueda ser implementado y operado con mayor precisión y efectividad, permitiendo que en lo futuro, conforme la universidad crezca en matrícula, estructura y dimensiones, ofrezca la posibilidad de llevar a cabo la administración y gestión de la información personal satisfaciendo lo exigido en la normatividad.

Así pues y con acuerdo a su MGO[93], la universidad se estructura hasta la fecha de seis unidades administrativas con sus respectivos objetivos y funciones, mismas que de alguna u otra manera y con base a lo establecido en el mismo MGO, son partícipes en alguna de las operaciones parte del tratamiento de datos

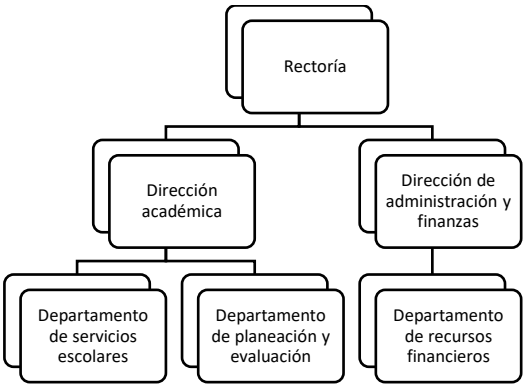
---

[92] A la fecha, UPTex cuenta con una matrícula de 1555 alumnos inscritos en los diferentes programas educativos tanto para la modalidad de licenciatura como de ingeniería. También a la fecha se encuentran adscritos a esta institución una plantilla docente de 61 profesores, mismos que imparten clases en las diferentes licenciaturas e ingenierías que ofrece la misma. Finalmente, el personal administrativo adscrito a la institución es la cantidad de 39 personas, mismos que se encuentran adscritos desde la oficina de rectoría hasta el personal de limpieza y mantenimiento.

[93] Manual General de Organización de la Universidad Politécnica de Texcoco, disponible en: *https://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/pdf/gct/2016/feb081.pdf*, consultado el 15 de octubre de 2019.

personales dentro de la institución, mismo organigrama y funciones que a continuación se representan y transcriben:

Figura 2. Organigrama de la Universidad Politécnica de Texcoco.



Fuente: Manual General de Organización de la Universidad Politécnica de Texcoco

a) Rectoría:

Proporcionar la información requerida para mantener actualizado el portal de Transparencia y Acceso a la Información Pública del Estado de México de la Universidad, así como atender en tiempo y forma las solicitudes de información correspondientes a su área, a través del sistema de acceso a la información mexiquense.

b) Dirección académica:

Diseñar e implementar los mecanismos de seguimiento de los alumnos que comprenda desde su ingreso, estancia y egreso de la Universidad.

c) Dirección de administración y finanzas:

Administrar las actividades relacionadas con la selección, ingreso, contratación, inducción, incidencias, desarrollo, capacitación, remuneraciones y demás prestaciones a que tiene derecho el personal administrativo y docente de la Universidad.

d) Departamento de servicios escolares:

Administrar, actualizar e instrumentar la base de datos para el registro, control y seguimiento de los alumnos inscritos en las carreras que ofrece la

Universidad, considerando los cambios y movimientos que se originen en el proceso de promoción, desde su ingreso hasta su egreso.

e) Departamento de planeación y evaluación:

Proponer e implantar un sistema que integre la matrícula escolar, así como los resultados de las funciones académico-administrativas, que permitan apoyar la toma de decisiones de Rectoría y, en su caso, realizar las correcciones pertinentes.

f) Departamento de recursos financieros:

Mantener el archivo resguardado de los documentos fuente, libros, registros y estados financieros de acuerdo a lo establecido por las leyes fiscales.

Como se ha podido apreciar, y con acuerdo a lo establecido en el MGO de la UPTex, todas las unidades administrativas partes de la institución llegan en determinado momento a realizar algún proceso de control y administración con base en los datos personales ya sea del alumnado, cuerpo docente o personal administrativo adscrito a la universidad configurándose de tal manera el denominado *tratamiento* de información personal conforme se establece en la normatividad en la materia, lo cual, como se ha venido postulando en el presente trabajo, debe de ser llevado a cabo en apego a los mecanismos de protección de datos personales como el SGDP que aquí se propone.

Ahora bien, un punto que se considera importante destacar, es el relativo a las funciones encomendadas al departamento de servicios escolares, pues como bien se puede apreciar, es en este departamento en el que llega a configurarse plenamente el *ciclo de vida* de los datos personales dentro de la universidad, pues es en este departamento en donde se da tratamiento a la información personal desde que los alumnos proporcionan sus datos personales al momento de la inscripción oficial, hasta el momento que egresan, sabiendo que con acuerdo a lo establecido en la ley, habrá de existir un periodo de resguardo de dicha información para finalmente eliminarla o suprimirla de sus bases de datos conforme lo recomienda la literatura al respecto.

Otra área que se considera importante resaltar dada la trascendencia de la información personal a la cual da tratamiento, es el departamento de administración y finanzas, pues es en este departamento en donde se recaba la información personal de toda la plantilla docente y administrativa que se encuentra adscrita a la universidad o que, en algún momento determinado, se ha postulado para ser parte de esta. Es decir, es el área en donde se concentra y se da tratamiento a información personal de los que actualmente laboran en este centro educativo, ya sea como personal administrativo o como docente.

Así entonces y no obstante todo lo previamente referido, resulta preciso mencionar que a la fecha la UPTex, como responsable de la protección de datos personales, *no cuenta aún con un SGDP* conforme se establece en la normatividad en la materia, situación que hace que el presente trabajo se considere oportuno y pertinente, ya que al contar con tal sistema, se colmaría lo instituido en el artículo 28 de la Ley local y diverso artículo 30 de la Ley general con relación al principio de responsabilidad que implica el deber de implementar políticas, programas y mecanismos obligatorios y exigibles al interior de la organización del responsable que acrediten el cumplimiento de los principios, deberes y obligaciones previstos en la normatividad de la materia, ya que la universidad al ser el responsable de la protección de datos personales, está obligado a la rendición de cuentas principalmente ante el titular y posteriormente ante el INAI e Infoem, según corresponda:

> Artículo 28. Entre los mecanismos que deberá adoptar el responsable para cumplir con el *principio de responsabilidad* establecido en la presente Ley están, al menos, los siguientes:
>
> …
>
> VII. Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, *sistemas* o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología *que implique el tratamiento de datos personales*, de conformidad con las disposiciones previstas en la presente Ley y las demás disposiciones legales aplicables.

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

Por otra parte, con fundamento en lo dispuesto por el artículo 94 de la Ley de protección de datos local, que establece que el Comité de Transparencia es la máxima autoridad en materia de protección de datos personales dentro de cada sujeto obligado y que tiene entre sus funciones la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho el derecho a la protección de datos personales en la organización del responsable, a continuación, se enlistan las funciones que dicho cuerpo colegiado tendrá con relación al SGDP que en su momento podría ser implementado dentro de la universidad:

1. Elaborar e implementar el SGDP en conjunto con las unidades y departamentos de la universidad.

2. Proponer cambios y mejoras al SGDP, a partir de la experiencia de su implementación.

3. Dar a conocer el SGDP al interior de la universidad

4. Coordinar la implementación del SGDP en las unidades y departamentos de la universidad.

5. Asesorar a las unidades y departamentos en la implementación del SGDP.

6. Presentar un informe mensual en el que describan las acciones realizadas para cumplir con lo dispuesto en el SGDP.

7. Supervisar la correcta implementación del SGDP.

8. Las demás que expresamente se señalen en el SGDP.

Es por todo lo anterior relatado que el SGDP que en el presente trabajo se propone, en su primera fase de diseño, habrá de proveer elementos y herramientas para que en etapas posteriores se proceda a implementar, aplicar, controlar y evaluar con el objetivo de proteger de manera sistemática y continua los datos personales y también, por otra parte, se pueda preservar la confidencialidad, integridad y disponibilidad de los datos personales que estén y lleguen a estar en posesión de la universidad, lo anterior con el propósito de colmar lo estipulado en el marco normativo aplicable a la materia y no ubicarse dentro de los supuestos legales de responsabilidades administrativas que, a guisa de ejemplo, a continuación se enlistan algunas de estas hipótesis:

> Artículo 165. Serán causas de responsabilidad administrativa de las y los servidores públicos por incumplimiento de las obligaciones establecidas en la presente Ley, las siguientes:
>
> …
>
> IV. No inscribir los sistemas de datos personales en el registro en el plazo que previene esta Ley.
>
> **…**
>
> IX. Incumplir el deber de confidencialidad establecido en esta Ley.
>
> …
>
> XV. Crear sistemas de datos personales y bases de datos en contravención a lo dispuesto en esta Ley.
>
> …
>
> XIX. Usar, sustraer, destruir, mutilar, ocultar, inutilizar, divulgar o alterar total o parcialmente y de manera indebida, datos personales que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión.

Son precisamenente las hipótesis previamente referidas las que en determinado momento pudieran actualizar un tipo de responsabilidad administrativa para el personal directivo de la universidad como sujeto obligado al no contar con un SGDP como se encuentra establecida la normatividad aplicable en la materia. Contar con un sistema mediante el cual el tratamiento de datos

personales se lleve a cabo de acuerdo al cuerpo jurídico relativo y aplicable generaría, por partida doble, una relativa tranquilidad y confianza tanto del personal interno de la institución como del cuerpo estudiantil, plantilla docente y personal administrativo adscritos a ella.

3.2 Descripción general del Sistema de Gestión de Datos Personales para la Universidad Politécnica de Texcoco

El SGDP que aquí se propone tiene como base, además de lo estipulado en la normatividad general y local en la materia, los parámetros de Autorregulación en materia de Protección de Datos Personales[94] y en las Recomendaciones en materia de seguridad de Datos Personales[95] sugeridos por el INAI y publicados en el Diario Oficial de la Federación el 30 de octubre de 2013, documentos que si bien no aplican a los sujetos obligados del sector público, se guarda congruencia con la postura técnica del instituto en el tema, organismo de mayor jerarquía en materia del derecho a la protección de datos personales.

3.2.1 El ciclo PHVA o círculo de Deming

El ciclo PHVA o círculo de Deming, es una estrategia basada en la mejora contínua de la calidad muy utilizado por los sistemas de gestión de la calidad, los sistemas de gestión ambiental y los sistemas de gestión de seguridad de la

[94] Parámetros de Autorregulación en Materia de Protecicón de Datos Personales, Diario Oficial de la Federación 29 de mayo de 2014, disponibles en: *https://www.economia.gob.mx/files/marco_normativo/PAR1.pdf*, consultados el 12 de octubre de 2019.

[95] Recomendaciones en materia de seguridad de Datos Personales, disponibles en: *https://www.dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013*, consultados el 12 de octubre de 2019.

información[96], misma herramienta que ha sido recomendada por el INAI y que invariablemente es utilizada en el diseño del SGDP que aquí se presenta.

Así entonces, el SGDP tendría que desarrollarse a lo largo de las siguientes cuatro fases: planificar, hacer, verificar y actuar (modelo PHVA), de acuerdo con lo establecido en la tabla siguiente:

Figura 1. Ciclo PHVA o Circuito Deming.

	Elemento	Fase del PHVA	Actividades
PROCESO	**Metas**	**P**lanificar	Se identifican políticas, objetivos, riesgos, planes, procesos y procedimientos necesarios para obtener el resultado esperado por el responsable o encargado (meta).
	Medios de acción	**H**acer	Se implementan y se hacen operar las políticas, objetivos, planes, procesos y procedimientos establecidos en la fase anterior.
		Verificar	Se evalúan y miden los resultados de lo implementado, a fin de verificar el adecuado funcionamiento del sistema de gestión y que se haya logrado la mejora esperada.
		Actuar	Se adoptan medidas correctivas y preventivas, en función de los resultados y de la revisión realizada, o de otras fuentes de información relevantes, para lograr la mejora continua.

Fuente: Parámetros de Autorregulación en materia de Protección de Datos Personales, 2013. INAI.

Para una comprensión más detallada del modelo anterior, a continuación, se proporciona más amplias explicaciones de cada fase:

1. Planear y establecer.

La primera fase se desarrolla a partir de definir los elementos necesarios para la operación del SGDP. De manera similar a un Sistema de Gestión de Seguridad de la Información (en adelante SGSI), resulta relevante contar con el alcance de la protección de datos, un documento formal donde se plasme el compromiso en este sentido, la definición de roles y responsabilidades para dar cumplimiento a los requisitos establecidos en las legislaciones. Además, se

[96] Ciclo de Deming. Disponible en: es.wikipedia.org/wiki/Ciclo_de _Deming, consultado el 12 de octubre de 2019.

recomienda contar con un inventario de los datos y posteriormente aplicar algún método para el análisis y evaluación de riesgos de seguridad. Posteriormente, es necesario definir las medidas de protección, de manera similar a una declaración de aplicabilidad.

2. Implementar y operar

La segunda fase se enfoca en la implementación de controles definidos para los riesgos identificados en la etapa anterior. A la vez, se debe desarrollar y ejecutar un plan de tratamiento de riesgos, con las diferentes opciones, así como la correspondiente aceptación y comunicación de riesgos residuales.

3. Monitorear y revisar

La tercera fase tiene como propósito revisar la operación del SGDP, así como su idoneidad y vigencia, especialmente si existen modificaciones en cuanto a los requisitos en las legislaciones, incidentes registrados, cambios en las políticas u objetivos de la organización. Las auditorías de seguridad son un elemento esencial en esta etapa, de manera similar a las que se realizan para un SGSI.

4. Mantener y mejorar

Con base en los resultados de la fase anterior, se deben tomar decisiones para realizar cambios, mejorar o mantener el SGDP, a través de acciones correctivas y otro tipo de iniciativas, como la capacitación del personal involucrado.

3.2.2 El ciclo de vida de los datos personales

Ahora bien, el tratamiento de datos personales que realicen las unidades y departamentos de la UPTex, deberá cumplir con los principios, deberes y obligaciones que establece la Ley local de protección de datos, para lo cual el SGDP que aquí se propone establecerá el marco de trabajo mínimo que se deberá seguir para alcanzar dicho objetivo.

En ese sentido, se recomienda que la UPTex adopte las mejores prácticas para la protección de datos personales en aquellos tratamientos que así lo

permitan y con acuerdo al nivel de desarrollo que exista. Para ello, se identificarán las obligaciones de datos personales que realicen las unidades y departamentos, con acuerdo a lo que establece la Ley local de protección de datos, y según el ciclo de vida de los datos personales.

En este punto es importante señalar que ni en la Ley General ni en la Ley local de protección de datos, ni en ningún otro cuerpo jurídico regulatorio en materia de protección de datos personales en México se hace expresa mención de lo que por ciclo de vida de los datos personales debe entenderse, siendo necesario remitirse a lo que la Agencia Española de Protección de Datos ha establecido en su Guía Práctica de Análisis de Riesgos en los tratamientos de datos personales sujetos al RGPD,[97] entendiendo dicha aplicabilidad al contexto europeo con base al Reglamento General de Protección de Datos, siendo el ciclo de vida de los datos personales el siguiente:

Figura 4. Ciclo de vida de los datos personales.

Fuente: Guía Práctica de Análisis de Riesgos en los tratamientos de datos personales sujetos al Reglamento General de Protección de Datos

- Captura de datos: Proceso de obtención de datos para su almacenamiento y posterior procesado. En esta categoría se pueden encontrar diversas

[97] "Ciclo de vida de los datos en materia de protección de datos (RGPD y LOPDGDD)", Iberley, 4 de febrero de 2019. Para mayor referencia al respecto, remitirse al sitio *https://www.iberley.es/temas/ciclo-vida-datos-materia-proteccion-datos-62740*, consultado el 15 de octubre de 2015.

técnicas: formularios web, formularios en papel, toma de muestras y realización de encuestas, grabaciones de audio y video, redes sociales, captación mediante sensores, etcétera.

- Clasificación / Almacenamiento: Establecer categorías y asignarlas a los datos para su clasificación y almacenamiento en los sistemas o archivos
- Uso / Tratamiento: Operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos de los datos automatizados o manuales.
- Cesión o transferencia de los datos a un tercero para su tratamiento: Traspaso o comunicación de datos realizada a un tercero, definido como aquella persona física o jurídica, pública o privada u órgano administrativo. Este concepto es muy amplio, puesto que recoge tanto la entrega, comunicación, consulta, interconexión, transferencia, difusión o cualquier otra forma de acceso a los datos.
- Destrucción: Eliminar los datos que puedan estar contenidos en los sistemas o archivos, de manera que no puedan ser recuperados de los soportes de almacenamiento.

Como bien se puede apreciar en la información ofrecida en el párrafo que antecede, el esquema del ciclo de vida de los datos personales se compone de los pasos previamente descritos, siendo el tercero al que expresamente se le denomina “uso o tratamiento”, sin embargo, el artículo 3, numeral XXXIII de la ley general establece que *tratamiento* es:

> Cualquier operación o conjunto de operaciones efectuadas mediante procedimeintos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Por lo tanto, y en estricto apego a lo que la ley general instituye, los cinco pasos que conforman el ciclo de vidad de los datos personales (captura, almacenamiento, tratamiento, transferencia y destrucción) en México son

considerados todos como tratamiento *per se,* y no solamente lo constituye la fase intermedia como se establece en la en Guía Práctica de Análisis de Riesgos en los tratamientos de datos personales sujetos al Reglamento General de Protección de Datos, observación que bien merece otro espacio y objeto de estudio.

3.2.3 El responsable dentro del sujeto obligado

Un punto de mayúscula importancia dentro de las políticas de protección de datos personales dentro de las instituciones u organizaciones ya sean del sector público o privado, es el relativo a la figura del *responsable* dentro del sujeto obligado a la protección de datos personales.

En ese sentido, el gobierno mexiquense ha diseñado e implementado diversos esquemas y políticas públicas gubernamentales a través del Infoem, como órgano garante de la protección de los datos personales en el Estado de México, que tienen como objetivos promover e impulsar el desarrollo de la cultura de protección de los datos personales y fortalecer el conocimiento, ejercicio y respeto por este derecho humano.

Así entonces, el gobierno estatal emitió el Programa Estatal y Municipal de Protección de Datos Personales teniendo como objetivo principal el reconocimiento y pleno ejercicio del derecho a la protección de los datos personales en el Estado de México, así como impulsar el desarrollo de la cultura de protección de los datos personales.

Este programa se dirige a los *responsables* del tratamiento de datos personales de la población de esta entidad, definidos en la Ley local de protección de datos, el cual tiene como visión constituirse como el instrumento rector de la política pública en materia de protección de los datos personales en la entidad.[98]

[98] Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios. Programa Estatal y Municipal de Protección de Datos Personales, disponible en:

Dicho programa se encuentra estructurado en ocho ejes temáticos, siendo los siguientes:

1. Educación y cultura de protección de los datos personales de los mexiquenses.
2. *Capacitación de los responsables.*
3. Certificación de los sujetos obligados.
4. Ejercicio de los derechos ARCO y la portabilidad.
5. Implementación y mantenimiento de los sistemas de gestión de seguridad.
6. Estándares en buenas prácticas en materia de protección de los datos personales.
7. Gestión de recursos
8. Monitoreo, seguimiento y verificación de metas.

Como puede ser apreciado, uno de los ejes temáticos que se abordan en el programa es el relacionado a la capacitación de los responsables de la protección de la información personal dentro de los sujetos obligados, figura que más está por decir, concentra neural importancia dentro de las estructuras de los sujetos obligados por ser la figura que se mantiene en diario y constante contacto con las decisiones con relación al ciclo de vida de los datos personales, identificándose, en el mismo documento, la siguiente problemática:

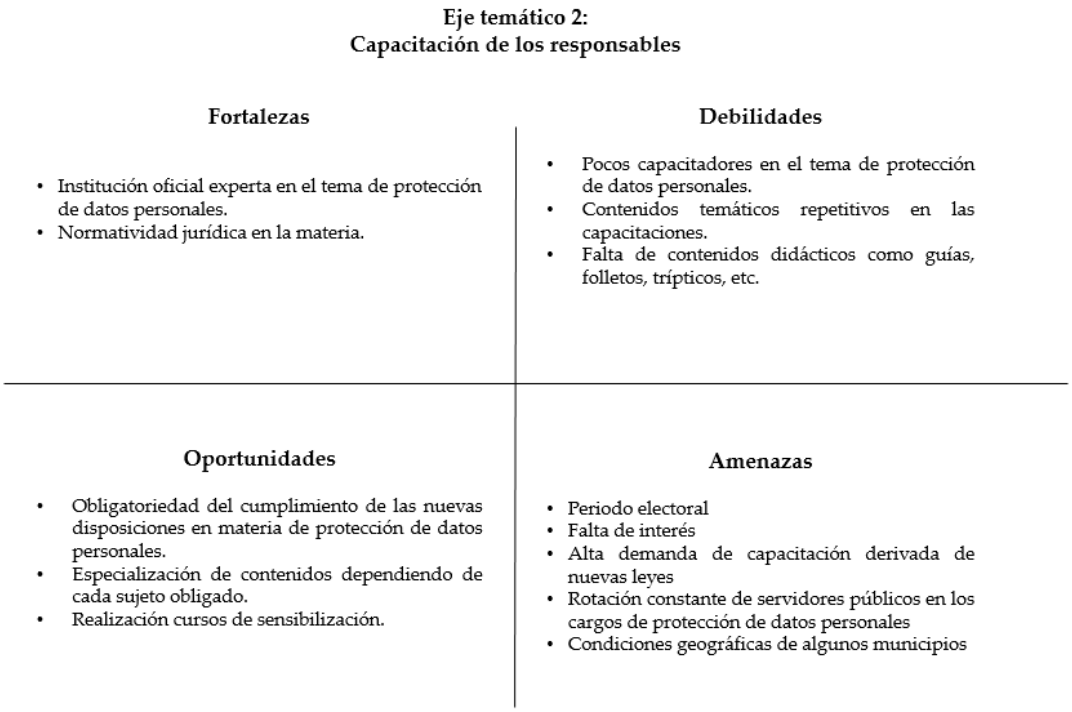
1. Falta de conocimiento y especialización por parte de los responsables respecto de los datos personales.
2. Necesidad de profesionalización integral de los responsables.
3. Riesgo de afectación del derecho a la protección de los datos personales.
4. Falta de certificación de los oficiales de Protección de Datos Personales.

---

http://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/pdf/gct/2018/may317.pdf, consultado el 16 de octubre de 2019.

En ese sentido, en el mismo documento se despliega un análisis FODA que pone de manifiesto la relevancia e importancia de la capacitación de dichos responsables como tarea fundamental del Infoem, el cual se presenta a continuación:

Figura 5. Análisis FODA en la capacitación de los responsables.



Fuente: Programa Estatal y Municipal de Protección de Datos Personales

Como bien puede apreciarse en el sector de oportunidades del análisis anterior, se menciona las amenazas derivadas de la falta de capacitación con motivo de la emisión de nuevas leyes en el entorno de la protección de datos personales tanto a nivel local como nacional. Pero no es sólo ello, pues bien es sabido que a nivel internacional también se formulan y emiten diversos documentos internacionales que, con el carácter de estándares, directrices o buenas prácticas se despliegan en torno al tema de la protección de la información personal, lo cual, sin duda, podría en mucho enriquecer y robustecer la protección de los datos personales en las organizaciones e instituciones tanto público como privadas.

También en ese sentido, existe otro cuerpo normativo con relación a la figura del responsable de sistemas de datos personales en posesión de sujetos obligados y la idoneidad del perfil del mismo, documento denominado "Recomendaciones para la designación de responsables de sistemas de datos personales en posesión de los sujetos obligados", el cual, con acuerdo al apartado de consideraciones del mismo documento, se establece que "tienen como propósito orientar a los Sujetos Obligados para que *una vez identificados los sistemas de datos personales* que están en su poder designen a los servidores públicos de las unidades administrativas que lo conforman que serán responsables del tratamiento de datos, tomando en cuenta las funciones establecidas en la propia Ley y el perfil laboral de los mismos". [99]

Así entonces, en el mismo cuerpo normativo se establece que a partir de las funciones que establece la Ley local de protección de datos, así como de la importancia que para la eficaz observancia del derecho a la protección de datos personales tiene la figura del responsable, se recomienda el siguiente perfil para la designación de este, mismo que a continuación se transcribe:

- Contar con conocimientos en la materia: es recomendable que la persona que tenga a su cargo la función de protección de los datos personales,

[99] Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios. Acuerdo mediante el cual se aprueban los lineamientos técnicos para la publicación, homologación y estandarización de la información establecida en el Título Quinto, capítulos II, II y IV, y el título Noveo de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios; adicional de aquella contemplada en el Título Quinto de la Ley General de Transparencia y Acceso a la Informaicón Pública, disponibles en *https://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/pdf/gct/2018/jun143.pdf*, consultados el 20 de octubre de 2019. [Las cursivas son propias]

tenga conocimiento sobre la materia, se interese en la misma y reciba capacitación constante.

- Contar con jerarquía dentro del Sujeto Obligado: es recomendable que el responsable cuente con la jerarquía o posición dentro del Sujeto Obligado ya que es la persona que debe responder por el cumplimento de la Ley y decidirá sobre el tratamiento de datos, así como el contenido y finalidad de los sistemas que custodiará y que se encuentran en poder de alguna unidad administrativa, por lo que se deberá procurar que dicho nombramiento recaiga, por lo menos, en el director de área u homólogo de la unidad administrativa que corresponda al interior del Sujeto Obligado.
- Aún y cuando la Ley de la materia no exige un nivel específico para la persona que sea designada responsable del sistema y el Sujeto Obligado tiene libertad para decidirlo; es indispensable que, por virtud de las funciones que desempeña, éste cuente con las facultades y capacidades suficientes para cumplirlas.
- Contar con recursos suficientes: es fundamental que la persona designada como responsable cuente con los recursos materiales, técnicos y humanos necesarios para el ejercicio de sus funciones y acciones, a efecto de cumplir las disposiciones previstas en la Ley, tomando en cuenta la naturaleza de los datos personales que trata.
- Contar con habilidades de organización y comunicación, así como visión y liderazgo. En virtud de que las funciones en materia de datos personales en muchas ocasiones serán de decisión, es indispensable que la persona que sea designada como responsable sea líder y escuchado en la unidad administrativa que custodia los sistemas de datos personales.

Con lo hasta aquí expuesto, se puede hacer constancia de la importancia que la figura del responsable dentro del sujeto obligado tiene en materia de protección de la información personal, ello con miras a potencializar y maximizar los recursos y energías que se puedan establecer al momento de desarrollar e implantar un SGDP dentro de la Universidad, ya que con acuerdo con lo establecido en la normatividad, se hace patente la seriedad de contar con el

personal adecuado para cubrir y atender las tareas propias en materia de protección de datos personales dentro de los sujetos obligados.

Ahora bien, una vez establecidas algunos antecedentes de carácter general, a continuación, se presentará de manera también generalizada los pasos que deberá de atender la universidad con el objetivo de implementar el SGDP que aquí se presenta en su diseño. Así pues, la estructura de un SGDP corresponderá a los siguientes pasos estructurales:

a) *Elaboración de diagnóstico del estado de cosas con relación a la protección de datos personales.* Para ello se propone el siguiente cuestionario que plantea de forma enunciativa, más no limitativa los siguientes cuestionamientos que habrán de aplicarse al personal directivo dentro de la universidad, cuestionario que, si bien es diseñado para aplicarse dentro de organizaciones del sector privado, auxilian y dan elementos para ser considerados en el sector público.

1) ¿Tiene la Universidad identificados al encargado, responsable, administrador y los operadores de las bases de datos de la institución?
2) ¿Tiene identificadas las bases de datos que maneja la Universidad?
3) ¿Sabe qué es el Infoem y la responsabilidad de la institución con el mismo?
4) ¿Tiene la Universidad una política de tratamiento y protección de datos personales conforme a la Ley General y Ley local de protección de datos?
5) ¿Qué tipo de datos personales reposan en las bases de datos de la universidad?
6) ¿Cuenta la universidad con medidas de seguridad de la información previamente establecidas?
7) ¿Cuenta la universidad con un sistema de gestión de la información implementado?
8) ¿Cuenta la universidad con un proceso de tratamiento y procesamiento de datos personales?
9) ¿Cuenta la universidad con la autorización de los titulares de los datos debidamente documentada?
10) ¿Transfiere, transmite o cede frecuentemente las bases de datos de la Universidad?

11) ¿Cuenta la Universidad con un sistema de gestión TIC y seguridad informática?
12) ¿Conoce las sanciones y supuestos de responsabilidad por no tener implementada una política de tratamiento de datos personales y/o registrar a tiempo las bases de datos de la universidad?

De esta forma y previo aplicado el cuestionario referido, se puede llegar a obtener una valoración más acercada a la realidad de la Universidad en materia de protección de datos personales y poder identificar con ello las principales deficiencias e insuficiencias en la materia y de ahí partir para la elaboración e implementación del SGDP. Hecho previamente el diagnóstico, se suceden una serie de pasos muy importantes a considerar e implementar de acuerdo al especialista en consultoría en protección de datos personales Jose Manuel Sanz[100]

> *b) Inventario de las bases de datos que incluyen datos personales.* Sin un análisis previo de la información que la Universidad dispone, es imposible valorar el alcance y la profundidad del SGDP. Es fundamental el adecuado inventario de esos tratamientos de datos y sus relaciones.
> *c) Procedimientos de seguridad.* La institución debe determinar para cada una de las estructuras de datos, cuáles son las medidas de seguridad más eficaces. Estas medidas deberán cubrir todos los aspectos de la vida útil de los datos: entradas, almacenamiento, gestión, cesiones y eliminación. Cada una de estas fases tiene que estar claramente delimitada.
> *d) Procedimientos organizativos.* Las personas son el elemento de salvaguarda más importante en la gestión de un SGDP. Todos los aspectos del tratamiento de los datos deben tener un responsable,

[100] Sanz, José Manuel, Consultoría en protección de datos, disponible en https://www.josemanuelsanz.es/, última fecha de consulta el 21 de octubre de 2019.

aunque puede ser el mismo para todos, que defina claramente que perfiles de usuario tienen acceso, que defina qué tipo de acceso, que límites tiene cada usuario, etcétera.

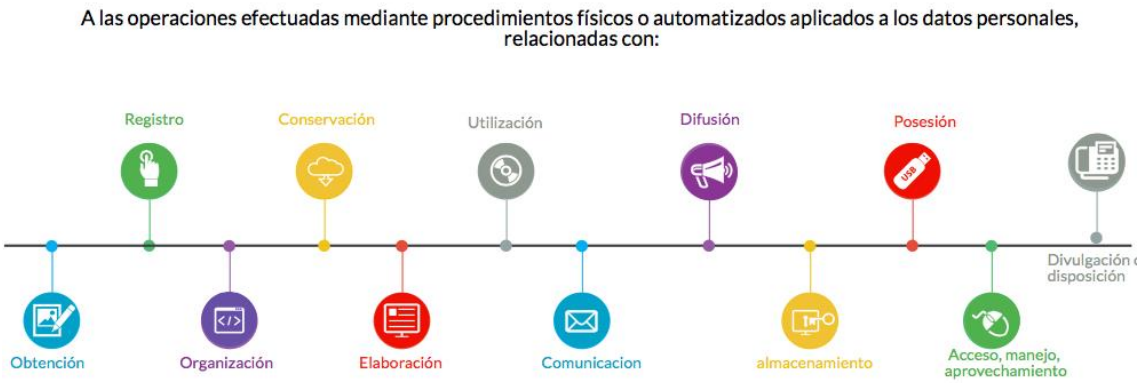
e) Identificación y gestión de riesgos e incidencias. La gestión preventiva de la seguridad, estableciendo procedimientos y responsables para cada área de la gestión de la información, permitirá un mayor control y una disminución de las incidencias en el uso de estos datos. Pese a todo, las incidencias son inevitables. Por ello el procedimiento que gestione estas incidencias, debe ser claro y conocido por toda la estructura a fin de poder dar respuesta a las mismas en el menor tiempo posible, acotando la incidencia a una fase del tratamiento y evitando que el resto de los procesos se vean afectados.

f) Procedimientos de formación y concienciación. Las personas son el principal recurso con el que cuenta un SGDP. Por ello, su adecuada formación en el uso de los datos y sus responsabilidades en ello es fundamental. La Universidad tiene que prever que el personal que tiene acceso y gestiona esta información, es consciente de la responsabilidad que asumen y de las consecuencias legales que supone una incidencia por mal uso de esta información

g) Procedimientos de respuestas de ejercicio de derecho. Los propietarios de los datos que la universidad gestiona pueden en todo momento ejercer los derechos que les son propios para tener la certeza de que su información está siendo gestionada como corresponde.

En ese sentido, la universidad tiene que disponer de los procedimientos, conforme a la normatividad aplicable, adecuados para dar respuesta a estos ejercicios de derechos y tienen que ser conocidos por todas aquellas personas que vayan a estar en contacto directo con los propietarios de los datos. Para ello, a continuación, se indican las operaciones que se le pueden dar a los datos personales y configurarse de esta forma el tratamiento que establece el artículo 4, numeral L, de la Ley local de protección de datos, siendo los siguientes:

Figura 6. Operaciones en el tratamiento de datos personales.



Fuente: Tomado de Davara F. de Marcos, Isabel, ""Adecuación legal en materia de protección de datos personales para la administración pública".[101]

3.3 Acciones específicas para el diseño del Sistema de Gestión de Datos Personales con base a la normatividad en materia de protección de datos personales en posesión de sujetos obligados del Estado de México y municipios

Como previamente se había establecido, gran parte de la literatura en materia de los mecanismos de gestión de seguridad de datos personales han sido propuestos por el INAI y en su momento, su antecesor el IFAI. No obstante este hecho, dicho material puede ser considerado para el diseño y mejora de actuales sistemas de gestión de datos personales dentro de las estructuras de los sujetos obligados, puesto que dicha literatura, como también previamente se estableció, puede aportar muy valiosos elementos técnicos en el diseño, implementación, control y evaluación de cualquier SGDP.

[101] Ponencia de Davara F. de Marcos, Isabel, "Adecuación legal en materia de protección de datos personales para la administración pública", en 2do Foro Internacional de Protección de datos personales y acceso a la información pública", el 7 de septiembre de 2017.

Así entonces, a continuación, se ofrece parte de las Recomendaciones en Materia de Seguridad de Datos Personales[102] que, como previamente se ha aclarado, se han diseñado para sistemas de seguridad de la información dentro de las organizaciones privadas, pero que, debido a su funcionalidad, operabilidad y factibilidad técnica, los mismos pueden ser aplicados a los SGDP de los sujetos obligados con la intención de ofrecer los niveles máximos de protección de la información personal.

En ese sentido, dichas recomendaciones se estructuran en cuatro fases y nueve pasos, mismos que se apegan a lo establecido en el denominado ciclo PHVA, como enseguida se muestra:

Fase 1. Planear el SGDP

Paso 1. Alcance y Objetivos. Consideraciones respecto al tratamiento de datos personales y el modelo de negocios de la organización.

Paso 2. Política de gestión de datos personales. El compromiso formal documentado de la Alta Gerencia hacia el tratamiento adecuado de datos personales en la organización.

Paso 3. Funciones y obligaciones de quienes traten datos personales. Asignación de responsabilidades para la implementación del SGDP.

Paso 4. Inventario de datos personales. Identificación de los tipos de datos y su flujo.

Paso 5. Análisis de Riesgo de los Datos Personales.

- Factores para determinar las medidas de seguridad. Conjunto de consideraciones que las organizaciones deben plantear como directrices para tratar el riesgo en función de sus alcances y objetivos.

---

[102] Recomendaciones en materia de seguridad de datos personales, 30 de octubre de 2013, disponibles en: *https://www.dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013*, consultados el 20 de octubre de 2019.

- Valoración respecto al riesgo. Proceso de ponderación para identificar los escenarios de riesgo prioritarios y darles tratamiento proporcional.

Paso 6. Identificación de las medidas de seguridad y análisis de brecha. Proceso de evaluación de las medidas de seguridad que ya existen en la organización contra las que sería conveniente tener. Los controles de seguridad, sin que sean limitativos, deben considerar los siguientes dominios:

- Políticas del SGDP
- Cumplimiento legal
- Estructura organizacional de la seguridad
- Clasificación y acceso de los activos
- Seguridad del personal
- Seguridad física y ambiental
- Gestión de comunicaciones y operaciones
- Control de acceso
- Desarrollo y mantenimiento de sistemas
- Vulneraciones de seguridad

Fase 2. Hacer e implementar el SGDP

Paso 7. Implementación de las medidas de seguridad aplicables a los datos personales.

- Cumplimiento cotidiano de medidas de seguridad. Consideraciones para el trabajo cotidiano con datos personales, así como el plan de tratamiento del riesgo de los activos relacionados a los mismos.

- Plan de trabajo para la implementación de las medidas de seguridad faltantes. Proceso en el que se decide y se implementa el tratamiento adecuado para un riesgo o grupo de riesgos respecto al contexto de la organización.

Fase 3. Verificar y monitorear el SGDP

Paso 8. Revisiones y auditoría. Proceso de revisión del funcionamiento del SGDP respecto a la política establecida, cada vez que exista un cambio en el contexto del alcance y objetivos del SGDP.

- Revisión de los Factores de Riesgo. Consideraciones para monitorear el estado del riesgo y aplicar las modificaciones pertinentes para mejorar el SGDP.

- Auditoría. Requerimientos para los procesos de auditoría interna/externa.

- Vulneraciones a la Seguridad de la Información. Consideraciones en caso de un incidente de seguridad.

Fase 4. Actuar y mejorar el SGDP

Paso 9. Mejora continua y capacitación. Consideraciones para incluir la protección de datos en la cultura de la organización y mantener siempre actualizado el SGDP.

- Mejora Continua. La aplicación de medidas preventivas y correctivas sobre el SGDP.

- Capacitación. Programas de mejora en la capacitación al personal para mantener la vigencia del SGDP.

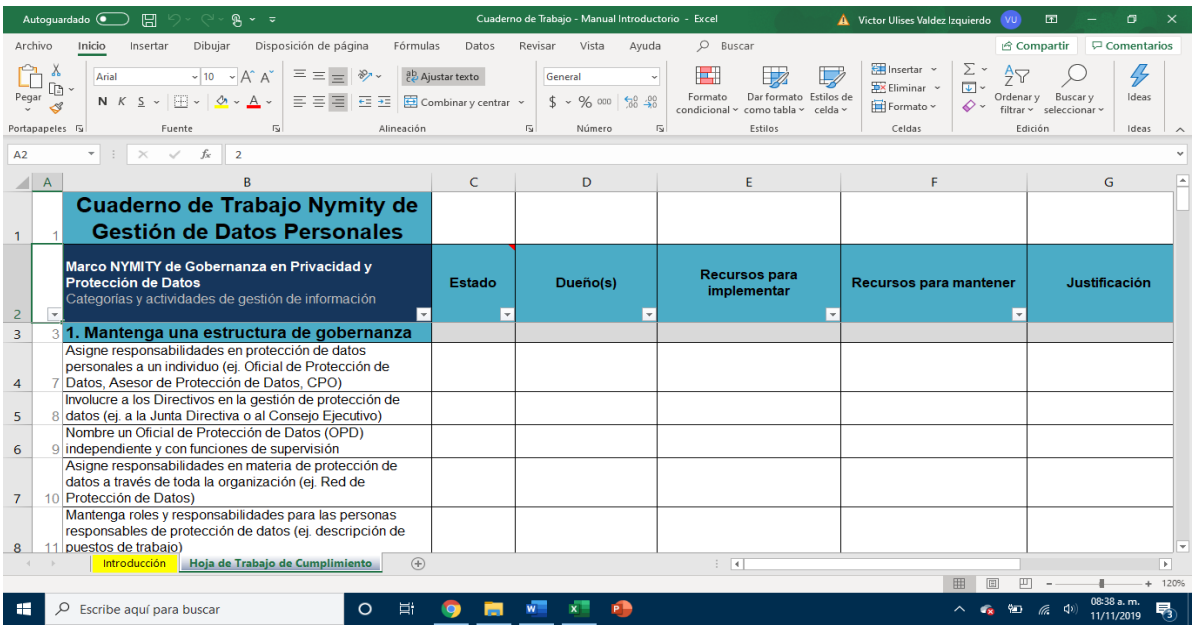
Por otra parte, existe disponible un cuaderno de trabajo[103] gratuito, consistente en un hoja de cálculo diseñado y elaborado por la organización NYMITY[104] que proporciona y ofrece herramientas bastante útiles y operacionales

[103] Cuaderno de trabajo descargable en: *https://latam.nymity.com/*, consultado el 20 de octubre de 2019.

[104] Con acuerdo a su página oficial, Nymity es la compañía global líder en investigación especializada en cumplimiento normativo y en la implementación y gestión efectiva de programas de protección de datos personales.
Esta herramienta de trabajo denominada “Cuaderno de Trabajo Nymity de Gestión de Datos Personales”, conforme lo expresa la misma organización, puede ser

al momento de iniciar la planeación del SGDP, puesto que el mismo ofrece diversos panoramas y escenarios en los que pudiera ubicarse las instituciones al momento de comenzar, gestionar e implementar el SGDP, mismo que no obstante haber sido diseñado para ser aplicado a la organizaciones dentro del sector privado, puede también ser retomado en ciertos puntos en las instituciones y dependencias del sector público.

Figura 7. Cuaderno de trabajo.



1	**Cuaderno de Trabajo Nymity de Gestión de Datos Personales**					
2	**Marco NYMITY de Gobernanza en Privacidad y Protección de Datos** Categorías y actividades de gestión de información	**Estado**	**Dueño(s)**	**Recursos para implementar**	**Recursos para mantener**	**Justificación**
3	**1. Mantenga una estructura de gobernanza**					
4	Asigne responsabilidades en protección de datos personales a un individuo (ej. Oficial de Protección de Datos, Asesor de Protección de Datos, CPO)					
5	Involucre a los Directivos en la gestión de protección de datos (ej. a la Junta Directiva o al Consejo Ejecutivo)					
6	Nombre un Oficial de Protección de Datos (OPD) independiente y con funciones de supervisión					
7	Asigne responsabilidades en materia de protección de datos a través de toda la organización (ej. Red de Protección de Datos)					
8	Mantenga roles y responsabilidades para las personas responsables de protección de datos (ej. descripción de puestos de trabajo)					

Fuente: Tomado de “Manual Nymity. Una aproximación estructurada a la gestión de datos personales”.

Tal cuaderno de trabajo se encuentra dividido en las siguientes actividades de gestión de la información más comunes que, como bien se podrá verificar, fue diseñado para satisfacer lo exigido en materia de protección de datos personales desde un entorno internacional:

---

utilizado en el presente trabajo puesto que el mismo no constituye ninguna forma de asesoría legal ni tiene fines de lucro ni será utilizado para fines comerciales, por lo puede ser libremente redistribuido en su totalidad, siempre y cuando las marcas, logos y la indicación de autor de Nymity no sean retirados, por lo que su autoría, el diseño del cuaderno de trabajo, sus logos y la marca son exclusiva propiedad de la compañía Nymity.

1) Mantener una estructura de gobernanza.

2) Mantener un inventario de datos personales.

3) Mantener una política de protección de datos.

4) Integrar la protección de datos en las operaciones.

5) Mantener un programa de capacitación y concientización.

6) Gestionar los riesgos de seguridad de la información.

7) Gestionar los riesgos con terceros.

8) Mantener avisos de privacidad.

9) Responder a las peticiones y quejas de los individuos.

10) Monitorear las nuevas prácticas operacionales.

11) Mantener un programa de gestión de incidentes y vulneraciones de datos.

12) Monitorear las prácticas de manejo de datos; y

13) Hacer seguimiento a criterios externos.

En ese mismo documento, dicha organización lanza una serie de planteamientos que bien valen la pena considerar al momento de iniciar la planeación de una política de gestión de datos personales dentro de los sujetos obligados, siendo los siguientes:

- ¿Tengo recursos limitados?
- ¿Soy nuevo/a en el área de gestión de protección de datos?
- ¿No logro encontrar un listado de requisitos que reúna todas mis necesidades?
- ¿Existe documentación limitada sobre la historia pasada de la gestión de protección de datos?
- ¿Cuento con un presupuesto limitado?
- ¿Cómo determino lo que ya está en marcha?
- ¿Cómo justificó la asignación de mayores recursos?

- ¿Cómo conservo los registros?
- ¿Cómo establezco y trabajo con un equipo de protección de datos que no trabaja para mí?
- ¿Cómo reporto el estado actual y el progreso de un programa?
- ¿Cómo le asigno responsabilidad a los demás?
- ¿Cómo demuestro el éxito del programa?

Así entonces, al momento de ir dando respuesta a este tipo de cuestionamientos, la Universidad podrá tener los elementos suficientes para determinar y establecer una política de gestión de la información personal lo más cercanamente posible a la realidad de los contextos en donde se encuentra ubicada y de esta manera también avizorar y advertir los posibles escenarios en la implantación del SGDP que aquí se propone en su diseño.

También, esta herramienta ofrece un cuadro que establece los recursos necesarios para implementar y mantener las tareas y actividades con motivo de la gestión de los datos personales dentro de la Universidad, el cual se transcribe enseguida:

Cuadro 3. Recursos del Programa de Protección de Datos.

Personas	**Procesos**	**Tecnología**	**Herramientas**
— Empleados - de tiempo completo o parcial — Aprobación o soporte de la Gerencia/ Directivos /Alta Dirección — Otros departamentos o grupos tales como Control interno/Cumplimiento/ ERM — Servicios compartidos (Seguridad de la Información, TI, Legal, Contratos) — Consultores Externos/Asesores/ Auditores/Servicios a	— Flujos de trabajo para aprobación — Monitoreo/ Mecanismo o controles de revisión — Comunicaciones/ Reuniones — Capacitación/Intercambio de conocimiento — Rutas de escalamiento de información	— Plataformas para compartir archivos/documentos — Herramientas de colaboración — Controles de protección de datos/seguridad de información — Sistemas EPR — Sistemas de expedición de tiquetes — Sistemas de entrenamiento en línea	— Suscripciones a sistemas de investigación para cumplimiento — Suscripciones a revistas para estar informado — Minutas y Modelos — Sistemas de gestión de datos personales — Software de reportes de cumplimiento en protección de datos /riesgos/ cumplimiento — Soluciones para PIA — Generadores de

Proveedores — Autoridad de Protección de Datos			cuadros comparativos de leyes — Soluciones para determinar puntos de referencia de cumplimiento

Fuente: Tomado de “Manual Nymity. Una aproximación estructurada a la gestión de datos personales”

Con elementos de la tabla anterior, será posible dimensionar en una forma más precisa y cierta los recursos humanos, tecnológicos y logísticos necesarios para implementar y en su momento controlar y evaluar el SGDP aquí propuesto, lo cual podrá permitir que la política de gestión de la información personal dentro de la Universidad sea dirigida conforme los parámetros y procedimientos apegados a la normatividad en la materia.

Finalmente, existe dentro de la normatividad en materia de protección de datos personales en el Estado de México otro cuerpo normativo de carácter técnico que se considera de obligada lectura y aplicación al momento de implementar el SGDP dentro de la institución, pues dicho documento contiene los lineamientos sobre medidas de seguridad aplicables a los sistemas de datos personales en posesión de los sujetos obligados,[105] mismos que pueden tener aplicación directa al momento de implementar y operar el SGDP aquí propuesto y que para efectos de referencia, a continuación se transcribe el contenido de manera general:

1. De los sistemas de datos personales
2. De las medidas de seguridad en el tratamiento de datos personales
3. De las medidas de seguridad para datos personales en soportes físicos

[105] 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, *op. cit*., nota 97.

4. De las medidas de seguridad para datos personales en soportes electrónicos
5. De las medidas de seguridad para transmisión de datos personales
6. De las medidas de seguridad para equipo de cómputo en zonas de acceso restringido
7. De las medidas de seguridad para asegurar continuidad y enfrentar desastres
8. De la documentación de medidas de seguridad en procesos y políticas de los sistemas de datos personales
9. De la verificación de los sistemas de datos personales por el Instituto
10. De la denuncia por violación a las disposiciones de la Ley.

Naturalmente, cada capítulo que previamente se ha referido, contempla una serie de secciones relativas al manejo, tratamiento, seguridad y protección de los datos personales en posesión de los sujetos obligados, mismo documento que debería de ser observado e implementado por el responsable de la implementación, control, administración y verificación del SGDP que aquí se ha propuesto.

3.4 Consideraciones finales al tercer capítulo

El desarrollo del presente capítulo ha tenido como objetivo principal el proporcionar los elementos y las herramientas fundamentales al momento de que se pretenda dar inicio al desarrollo e implementación de un sistema de gestión de datos personales dentro de la Universidad Politécnica de Texcoco, mismo que conforme a la normatividad aplicable a la materia tendrá que satisfacer y colmar lo establecido y requerido en la normatividad aplicable a la materia.

Como también pudo relatarse y constatarse, la consecución de esta empresa representará una efectiva sinergia de voluntades, capacidades, recursos y estrategias dentro de la universidad, ya que tal tarea implica y significa una

perspectiva multilateral al interior de la institución al tener obligatorio la participación de todo el personal que de alguna u otra forma lleva a cabo alguna operación parte del tratamiento de datos personales.

Desde la participación de la parte rectora y directiva de la universidad, pasando sustancialmente por las áreas y unidades administrativas parte de la estructura de la misma, hasta la inclusión del personal operativo e incluso la plantilla docente, todos ellos serán parte de un sistema global en relación a la protección de datos personales conforme se ha propuesto en el presente trabajo, puesto que si en determinado momento alguna de las piezas integrantes de este sistema no cumple o no satisface lo establecido en el conjunto del sistema, el mismo podría perder su efectividad y funcionalidad.

Conclusiones

Conclusiones

A lo largo de esta investigación el objetivo que se persiguió fue diseñar de manera general, un sistema de gestión de datos personales para que pudiera ser implementado en la Universidad Politécnica de Texcoco, toda vez que se identificó que dicha institución es un sujeto obligado a insituir esta herramienta por mandato de ley y sin embargo aún no cuenta con el, situación que se observa riesgosa ya que coloca a la institución en un incumplimiento a la norma jurídica y por consiguiente puede hacerse acreedora a las sanciones previstas para los sujetos en inclumplimiento de el marco normativo en la materia.

Si bien es cierto existe el riesgo de ser sancionado, lo más importante en el tema planteado no es este específicamente, sino que los individuos que conforman la comunidad de la institución universitaria se encuentran vulnerables ante el desconocimiento y falta de un sistema de gestión de datos personales que cumpla con estándares de seguridad en todo el abanico de actividades que incluye el tratamiento de sus datos.

Así, tomando en consideración la relevancia del tema, y el objetivo general de la investigación se inició el trabajo elaborando el marco teórico conceptual en rededor del tema para comprender qué elementos son los que integran el sistema propuesto y los limites o dificultades que se pudieran encontrar en el diseño. De este modo se definió el concepto de dato personal, sujeto obligado, e incluso universidad públcia para dotar de certeza conceptual al resto del trabajo y reconoder cuáles son las categorías elementales del trabajo de investigación.

En una segunda etapa se analizaron todos y cada uno de los cuerpos normativos que rodean la temática desde el contexto nacional en la incorporación del derecho de protección de datos personales incluídos a nivel constitucional, la Ley General de Protección de Datos y la local del estado de México, pasando por los estándares internacionales que van desde las Declaraciones de la Asamblea General de las Naciones Unidas hasta documentos elaborados por organismo internacionales e inclusive legislación de otros Estados que permitan complementar aquellos vacíos que se encuentran aún en las normas mexicanas tal es el caso de por ejemplo el concepto de ciclo de vida de los datos personales,

que si bien reconocemos en México en la práctica, en la normatividad en la materia no se encuentra aún contemplado.

Finalmente en la tercera parte de esta investigación se procedió al diseño del sistema de gestión de datos personales para la institución universitaria, tomando elementos de sistemas de análisis como el modelo PHVA,(planificar, hacer, verificar y actuar) así como la identificacón de elementos FODA (fortalezas, oportunidades, desafíos y amenazas), para que por medio de cuestionarios, y herramientas tecnológicas como la que proporciona la empresa Nymity que es la compañía global líder en investigación especializada en cumplimiento normativo y en la implementación y gestión efectiva de programas de protección de datos personales evidentemente con las adaptaciones a las necesidades de la institución universitaria objeto de esta investigación.

En general los elementos que integran el sistema de gestión de protección de datos personales incluye los siguientes apartados: 1) De los sistemas de datos personales; 2) De las medidas de seguridad en el tratamiento de datos personales; 3) De las medidas de seguridad para datos personales en soportes físicos; 4) De las medidas de seguridad para datos personales en soportes electrónicos; 5) De las medidas de seguridad para transmisión de datos personales; 6) De las medidas de seguridad para equipo de cómputo en zonas de acceso restringido; 7) De las medidas de seguridad para asegurar continuidad y enfrentar desastres; 8) De la documentación de medidas de seguridad en procesos y políticas de los sistemas de datos personales; 9) De la verificación de los sistemas de datos personales por el Instituto; 10) De la denuncia por violación a las disposiciones de la Ley.

En esta ocasión no se profundizó en cada uno de estos puntos ya que antes de que se pueda desarrollar cada fase del sistema es necesario que las autoridades universitarias aprueben esta propuesta ya que sin ello, sería por demás ocioso avanzar en el diseño del sistema si es que no se aprueba su implementaicón, por ello sirva hasta aquí el trabajo de investigación aplicada para solucionar el tema de la falta de un sistema de gestión de datos personales para la

Universidad Politécnica de Texcoco en la espera de que pronto pueda darse continuidad a la fase dos de este proyecto.

Bibliografía

ARROYO KALIS, Juán Ángel, "*Habeas data:* elementos conceptuales para su implementación en México" [en línea], México, Instituto de Investigaciones Jurídicas de la UNAM, disponible en: *https://archivos.juridicas.unam.mx/www/bjv/libros/10/4633/4.pdf*, última fecha de consulta el 31 de octubre de 2019.

BAÑO, Rodrigo, "¿Qué es una Univerisidad Pública?, [en línea] Universidad de Chile, Facultad de Ciencias Sociales, disponible en *http://www.facso.uchile.cl/noticias/67245/que-es-una-universidad-publica*, última fecha de consulta 21 de julio de 2019.

BARINAS UBIÑAS, Désirée, "El impacto de las Tecnologías de la Información y de la Comunicación en el derecho a la vida privada: las nuevas formas de ataque a la vida privada", *Revista Electrónica de Ciencia Penal y Criminología* [en línea], núm. 15 vol. 9septiembre de 2013, disponible en: *http://criminet.ugr.es/recpc/15/recpc15-09.pdf*, fecha de consulta 10 de agosto de 2019.

CABALLERO, José Antonio, *et. al.*, "El futuro del Instituto Federal de Acceso a la Información Pública y Protección de Datos Personales: consideraciones sobre su autonomía constitucional" [en línea], *Revista electrónica*, núm. 7, 2012, disponible en *https://archivos.juridicas.unam.mx/www/bjv/libros/7/3196/1.pdf*, última fecha de consulta el 28 de agosto de 2019.

CARTA DE LA ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Disponible en: *http://www.oas.org/es/sla/ddi/tratados_multilaterales_interamericanos_A-41_carta_OEA.asp*, última fecha de cosnulta el 31 de octubre de 2019.

CÉDRIC LAURANT CONSULTING AND PRIVACY, "Guía de privacidad para hispanoparlantes 2012" [en línea], Privacy International, disponible en: *https://issuu.com/cedriclaurant/docs/120101-guia_privacidad_2012-clc_pi-c*. [Las cursivas son propias], última fecha de consulta el 31 de octubre de 2019.

CELIS QUINTAL, Marcos Alejandro, "La protección de la intimidad como derecho fundamental de los mexicanos" [en línea], en Cienfuegos Salgado, David y Macías Vázquez María Carmen (coords.), *Estudios en homenaje a Marcia Muñoz de Alba Medrano*. *Protección de la persona y derechos fundamentales*, México, 2006, disponible en: *https://dialnet.unirioja.es/servlet/autor?codigo=2032970*, última fecha de consulta el 31 de octubre de 2019.

Ciclo de vida de los datos en materia de protección de datos (RGPD y LOPDGDD), Iberley, 4 de febrero de 2019. Para mayor referencia al respecto, remitirse al sitio *https://www.iberley.es/temas/ciclo-vida-datos-materia-proteccion-datos-62740*, consultado el 15 de octubre de 2015.

CÓDIGO CIVIL FEDERAL, disponible en: *http://www.diputados.gob.mx/LeyesBiblio/pdf/2_030619.pdf*, última fecha de consulta el 31 de octubre de 2019.

COMUNICADO DEL INAI [en línea] de fecha 4 de enero de 2018, titulado: *Garantiza INAI a titulares el acceso a datos personales resguardados por instituciones educativas*, disponible en: *https://www.mugsnoticias.com.mx/noticias-del-dia/garantiza-inai-a-titulares-el-acceso-a-datos-personales-resguardados-por-instituciones-educativas/*, última fecha de consulta el 31 de octubre de 2019.

CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS [en línea], disponible en: *http://www.diputados.gob.mx/LeyesBiblio/pdf/1_060619.pdf*, última fecha de consulta el 31 de octubre de 2019.

CONVENCIÓN AMERICANA DE DERECHOS HUMANOS [en línea], disponible en: *http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/D1BIS.pdf*, última fecha de consulta el 20 de julio de 2019.

CONVENIO EUROPEO DE DERECHOS HUMANOS [en línea], disponible en: *https://www.echr.coe.int/Documents/Convention_SPA.pdf*, última fecha de consulta el 20 de julio de 2019.

CRISTEA UIVARU, Lucia Nicole, "La protección de datos de carácter sensible en el ámbito europeo. Historia clínica digital y big data en salud" [en línea], tesis doctoral, Universitat Abat Oliba CEU, 2017, disponible en: *https://www.tdx.cat/bitstream/handle/10803/442972/Tlcu.pdf?sequence=1&isAllowed=y*, última fecha de consulta el 31 de octubre de 2019.

CUADERNO DE TRABAJO descargable en: *https://latam.nymity.com/*, consultado el 20 de octubre de 2019.

DECLARACIÓN UNIVERSAL DE LOS DERECHOS HUMANOS [en línea], disponible en: *https://www.ohchr.org/en/udhr/documents/udhr_translations/spn.pdf*, fecha de consulta 20 de julio de 2019.

DECRETO DEL EJECUTIVO DEL ESTADO DE MÉXICO POR EL QUE SE CREA EL ORGANISMO PÚBLICO DESCENTRALIZADO DE CARÁCTER ESTATAL DENOMINADO UNIVERSIDAD POLITÉCNICA DE TEXCOCO, disponible en: *http://uptexcoco.edomex.gob.mx/sites/uptexcoco.edomex.gob.mx/files/files/Acta_Decreto%20de%20creaci%C3%B3n%20UPTex.pdf*, última fehca de consulta el 30 de agosto de 2019.

DECRETO NÚMERO 209 POR EL QUE SE EXPIDE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DEL ESTADO DE MÉXICO Y MUNICIPIOS, disponible en: *https://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/pdf/gct/2017/may305.pdf*, última fecha de consulta el 31 de octubre de 2019.

DÍAZ REVORIO, Francisco Javier, *Los derechos humanos ante los nuevos avances científicos y tecnológicos. Genética e internet ante la Constitución,* México, Tirant lo Blanch-Comisión Nacional de Derechos Humanos, 2009.

ESCALANTE GONZALBO, Fernando, *El derecho a la privacidad*, Cuadernillos de transparencia, México, Instituto Federal de Acceso a la Información Pública (IFAI), núm. 2, 2008.

ESTÁNDARES DE PROTECCIÓN DE DATOS PERSONALES, Red Iberoamericana de Protección de Datos, 2017, disponible en: *http://www.redipd.es/la_red/Historia/index-ides-idphp.php*, última fecha de consulta el 31 de octubre de 2019.

EXPOSICIÓN DE MOTIVOS DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE MÉXICO, disponible en: *https://seduc.edomex.gob.mx/sites/seduc.edomex.gob.mx/files/files/acerca/Marco%20Juridico/Ley%20de%20Protecci%C3%B3n%20de%20Datos%20Personales%20del%20Estado%20de%20M%C3%A9xico.pdf*, última fecha de consulta el 3 de septiembre de 2019.

FERNÁNDEZ DE MARCOS, Isabel Davara, "Protección de datos de carácter personal en México: problemática jurídica y estatus normativo actual", en Compendio de lecturas y legislación. Protección de datos personales, México, Tiro Corto Editores, 2010.

GALDÓN CLAVELL, Gemma, "¿Qué hacen con nuestros datos en intenet?", *El país* [en línea], junio 2015, disponible en: *https://elpais.com/tecnologia/2015/06/12/actualidad/1434103095_932305.html*, última fecha de consulta 18 de julio de 2019.

GARCÍA GONZÁLEZ, Aristeo, "La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado", Boletín Mexicano de Derecho Comparado, nueva serie [en línea], año XI, núm. 120, septiembre-diciembre, 2007, México, Instituto de Investigaciones Jurídicas de la UNAM, disponible en *http://transparencia.udg.mx/sites/default/files/La%20protecci%C3%B3n%20de%20datos%20personales%20derecho%20fundamental%20del%20siglo%20XXI.%20un%20estudio%20comparado.pdf*, última fecha de consulta el 1 de agosto de 2019.

GARZÓN VALDÉS, Ernesto, *Lo íntimo, lo privado y lo público*, Cuadernillos de transparencia, México, Instituto Federal de Acceso a la Información Pública (IFAI), núm. 6, 2008.

GUERRA FORD, Oscar M., "Las legislaciones de protección de datos personales en el país", en *Retos de la protección de datos personales en el sector público* [en línea], México, Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, México, 2011, disponible en: *http://www.infodf.org.mx/comsoc/campana/2012/LIbrodatosPweb.pdf*, última fecha de consulta el 19 de agosto de 2019.

INFORME DEL COMITÉ JURÍDICO INTERAMERICANO DE LA OEA SOBRE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES, de fecha 26 de marzo de 2016 [en línea], disponible en: *http://www.redipd.es/documentacion/otrosdocumentos/common/Informe_CJI-*

doc_474-15_rev2_26_03_15.pdf, última fecha de consulta el 15 de agosto de 2019.

INICIATIVA CON PROYECTO DE DECRETO POR LA QUE SE EXPIDE LA LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS, Salón de Sesiones del Pleno del Senado de la República, 30 de abril de 2015, disponible en: *http://www.senado.gob.mx/comisiones/gobernacion/docs/proteccion_datos/Iniciativa.pdf*, última fecha de consulta el 31 de octubre de 2019.

INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE MÉXICO Y MUNICIPIOS. PROGRAMA ESTATAL Y MUNICIPAL DE PROTECCIÓN DE DATOS PERSONALES, disponible en: *http://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/pdf/gct/2018/may317.pdf*, consultado el 16 de octubre de 2019.

INSTITUTO FEDERAL DE ACCESO A LA INFORMACIÓN PÚBLICA, "Guía práctica para ejercer el derecho a la protección de datos personales", México, 2015.

INSTITUTO NACIONAL DE ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES (INAI), "Introducción a la Ley General de protección de datos personales en posesión de sujetos obligados: manual del participante", México, 2017, disponible en: *http://www.ift.org.mx/sites/default/files/anexo_circular_10-18_manual_lgpdppso_acc.pdf*. [Las cursivas son propias], última fecha de consulta el 31 de octubre de 2019.

KATZ, Jorge, "Los caminos hacia una sociedad de la información en América Latina y el Caribe", Comisión Económica para América Latina y el Caribe (CEPAL), disponible para su consulta en: *https://repositorio.cepal.org/bitstream/handle/11362/2354/2/S034237_es.pdf*, última fecha de consulta, el 17 de julio de 2019.

LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS página oficial, disponible en: *http://www.redipd.es/la_red/Historia/index-ides-idphp.php* [Las cursivas son propias], última fecha de consulta el 31 de octubre de 2019.

LEFRANC WEEGAN, Federico César, *Terra incógnita. Bases para una política criminal pro persona en la sociedad digital* [en línea], Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación (INFOTEC), México, 2015, disponible en: *https://www.infotec.mx/work/models/infotec/biblioteca/25/25.pdf*, última fecha de consulta el 31 de octubre de 2019.

LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DEL ESTADO DE MÉXICO Y MUNICIPIOS, Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios, julio de 2017, disponible en: *https://www.infoem.org.mx/doc/publicaciones/LeyDeDatosPersonales.pdf*, última fecha de consutla el 1 de septiembre de 2019.

LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS, disponible en: *http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf*, últma fecha de consulta el 29 de agosto de 2019. [Las cursivas son propias].

LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS, disponible en: *http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf*, última fecha de consulta el 31 de octubre de 2019.

LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA, disponible en: *http://www.diputados.gob.mx/LeyesBiblio/pdf/LGTAIP.pdf*, última fecha de consulta el 31 de octubre de 2019.

LINEAMIENTOS POR LOS QUE SE ESTABLECEN LAS POLÍTICAS, CRITERIOS Y PROCEDIMIENTOS QUE DEBERÁN OBSERVAR LOS SUJETOS OBLIGADOS, para proveer la aplicación e implementación de la Ley de Protección de Datos Personales del Estado de México, disponibles en: *https://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/vigentes/may031.PDF*, última fecha de consulta el 3 de septiembre de 2019.

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, disponible en: *https://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/vigentes/may083.PDF*, última fecha de consulta el 4 de septiembre de 2019.

LÓPEZ CARBALLO, Daniel A. (coord.), "Protección de datos y habeas data: una visión desde Iberoamérica" [en línea], con motivo de la XVIII Edición del Premio Protección de Datos Personales de Investigación, España, Agencia Española de Protección de Datos, 2105, disponible en: *http://bgbg.mx/wordpress/wp-content/uploads/2015/06/Proteccion_de_datos_y_habeas_data.pdf*, última fecha de consulta el 31 de octubre de 2019.

MANUAL GENERAL DE ORGANIZACIÓN DE LA UNIVERSIDAD POLITÉCNICA DE TEXCOCO, disponible en: *https://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/pdf/gct/2016/feb081.pdf*, consultado el 15 de octubre de 2019.

MAQUEO RAMÍREZ, María Solange y MORENO, Jimena, "Implicaciones de una ley general en materia de protección de datos personales", en *Revista especializada del Centro de Investigación y Docencia Económica* (CIDE) [en línea], núm. 64, disponible en: *https://docplayer.es/19273602-Maria-solange-maqueo-y-jimena-moreno.html*, última fecha de consulta el 28 de agosto de 2019.

MAQUEO RAMÍREZ, María Solange, *et. al*., "Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario" [en línea], en *Revista de Derecho Valdivia*, volumen XXX, núm. 1,

disponible en: *https://scielo.conicyt.cl/pdf/revider/v30n1/art04.pdf*, última fecha de consulta el 17 de agosto de 2019.

MILLÁN GÓMEZ, Agustín, "Reconocimiento normativo del derecho a la protección de datos personales en el ámbito internacional", *en Retos de la protección de datos personales en el sector público* [en línea], México, Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal (InfoDF), disponible en: *http://www.infodf.org.mx/comsoc/campana/2012/LIbrodatosPweb.pdf*, última fecha de consulta el 31 de octubre de 2019.

OCDE, "Perspectivas de la OCDE en ciencia, tecnología e innovación 2016 (Extractos): América Latina", París, OCDE, disponible en: *https://www.oecd-ilibrary.org/docserver/9789264303546-es.pdf?expires=1565822308&id=id&accname=guest&checksum=C0FDBAEEB11CCBD61FE752DFCC735E79*, última fecha de consulta el 31 de octubre de 2019.

ORGANIZACIÓN DE LAS NACIONES UNIDAS, Asamblea General, "El derecho a la privacidad en la era digital", 31 de octubre de 2016, disponible en: *https://www.acnur.org/fileadmin/Documentos/BDL/2017/10904.pdf*, última fecha de consulta el 22 de octubre de 2019.

ORNELAS NÚÑEZ, Lina y López Ayllón, Sergio, "La recepción del derecho a la protección de datos en México: breve descripción de su origen y estatus legislativo", en *Protección de datos personales. Compendio de lecturas y legislación*, México, Tiro Corto Editores, 2010.

PACTO INTERNACIONAL DE DERECHOS CIVILES Y POLÍTICOS [en línea], disponible en: *http://www.corteidh.or.cr/tablas/3769.pdf*, última fecha de consulta el 20 de julio de 2019.

PÁGINA OFICIAL DE LA ONG "Derechos Digitales", disponible en: *https://www.derechosdigitales.org/quienes-somos/derechos-digitales/*, última fecha de consulta el 31 de octubre de 2019.

PÁGINA OFICIAL DEL INAI, disponible en: *http://inicio.inai.org.mx/SitePages/que-es-el-inai.aspx*, última fecha de consulta el 28 de agosto de 2019.

PARÁMETROS DE AUTORREGULACIÓN EN MATERIA DE PROTECICÓN DE DATOS PERSONALES, Diario Oficial de la Federación 29 de mayo de 2014, disponibles en: *https://www.economia.gob.mx/files/marco_normativo/PAR1.pdf*, consultados el 12 de octubre de 2019.

PESCHARD MARISCAL, Jaqueline, "El Instituto Federal de Acceso a la Información Pública como órgano garante en materia de Protección de Datos Personales", en *Protección de datos personales. Compendio de lecturas y legislación*, México, Tiro Corto Editores, 2010.

PIÑAR MAÑAS, José Luis, "¿Existe privacidad?", en H. Cámara de Diputados, *Protección de datos personales: compendio de lecturas y compilación* [en línea], México, Tiro Corto Editores, 2010, disponible en:

http://www.transparencia.udg.mx/sites/default/files/Protecci%C3%B3n%20de%20datos%20personales.%20Compendio%20de%20lecturas%20y%20legislaci%C3%B3n.pdf, última fecha de consulta el 31 de octubre de 2019.

PONENCIA DE DAVARA F. DE MARCOS, Isabel, "Adecuación legal en materia de protección de datos personales para la administración pública", en 2do Foro Internacional de Protección de datos personales y acceso a la información pública", el 7 de septiembre de 2017.

PRESENTACIÓN AL LIBRO "Protección de datos personales. Compendio de lecturas y legislación", México, Tiro Corto Editores, 2010.

PRINCIPIOS DE LA OEA sobre la privacidad y la protección de datos personales, Organización de los Estados Americanos, disponible en: *http://www.redipd.es/documentacion/otrosdocumentos/common/Informe_CJI-doc_474-15_rev2_26_03_15.pdf*, última fecha de consulta el 31 de octubre de 2019.

PROGRAMA ESTATAL DE PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE MÉXICO, disponible en: *http://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/pdf/gct/2018/may317.pdf*, última fecha de consulta el 3 de septiembre de 2019.

PUENTE DE LA MORA, Ximena, "Reforma al artículo 6 constitucional que considera el acceso a la información como derecho fundamental en México, retos y perspectivas" *Revista de Derecho Informático* [en línea], núm. 139, 2010, disponible en: *http://www.alfa-redi.org/sites/default/files/articles/files/puente_2.pdf*, última fecha de consulta el 25 de agosto de 2019.

REAL ACADEMIA ESPAÑOLA, disponible en: *https://dle.rae.es/?id=Bskzsq5|BsnXzV1*, última fecha de consulta el 31 de octubre de 2019.

RECOMENDACIONES EN MATERIA DE SEGURIDAD DE DATOS PERSONALES, 30 de octubre de 2013, disponibles en: *https://www.dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013*, consultadas el 20 de octubre de 2019.

REGLAMENTO (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), disponible en: *https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679*.

REGLAMENTO DE LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS [en línea], disponible en *http://www.redipd.es/documentacion/common/REGLAMENTO_RIPD_DIC2018.pdf,* última fecha de consulta el 16 de agosto de 2019.

SÁNCHEZ HERNÁNDEZ, Luis Ricardo, “Sistematización de obligaciones en materia de protección de datos personales para el sector público en el Estado de México”, [en línea], *Tesis de maestría en Derecho de las Tecnologías de la Información y Comunicación*, Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación (INFOTEC), Ciudad de México, 2017, disponible en: *https://infotec.repositorioinstitucional.mx/jspui/handle/1027/2*, última fecha de consulta el 1 de septiembre de 2019.

SÁNCHEZ TORRES, Jenny Marcela, *et.al.*, *“*La sociedad de la información: Génesis, iniciativas, concepto y su relación con Las TIC” [en línea], *Revista UIS Ingenierías*, Colombia, vol. 11, núm. 1, enero-junio, 2012, disponible en: *http://www.redalyc.org/articulo.oa?id=553756873001*, última fecha de consulta el 31 de octubre de 2019.

SANZ, JOSÉ MANUEL, Consultoría en protección de datos, disponible en https://www.josemanuelsanz.es/, última fecha de consulta el 21 de octubre de 2019.

SITIO OFICIAL DE LA CUMBRE MUNDIAL DE LA SOCIEDAD DE LA INFORMACIÓN, CMSI-ONU, disponible en: *https://www.itu.int/net4/wsis/forum/2019/es/* [Las cursivas son propias], última fecha de consulta el 18 de julio de 2019.

SITIO OFICIAL DE LA ORGANIZACIÓN PARA LA COOPERACIÓN Y DESARROLLO ECONÓMICOS (OECD), disponible en: https://www.oecd.org/centrodemexico/laocde/, [Las cursivas son propias], última fecha de consulta el 13 de agosto de 2019.

SITIO OFICIAL DE LA RIPDP, disponible en *http://www.redipd.es/la_red/Historia/index-ides-idphp.php*, última fecha de consulta el 16 de agosto de 2019.

SITIO OFICIAL DE PRIVACIDAD INTERNACIONAL, PRIVACY INTERNATIONAL, disponible en: https://privacyinternational.org/es/about, última fecha de consulta el 18 de julio de 2019.

SITIO OFICIAL DEL INFOEM, disponible en: *http://www.infoem.org.mx/src/htm/poderEjecutivo.html*, última fecha de consulta el 30 de agosto de 2019.

SOLOVE, Daniel J., “Undertandig privacy” [en línea], *George Washington Universiti Law School, Public Law & Legal Theory Research Paper Series*, paper núm. 420, 2008, disponible en: *http://ssrn.com/abstract=1127888*, consultado el 19 de julio de 2019.

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, Contradicción de Tesis 293/2011, disponible en: *http://www2.scjn.gob.mx/asuntosrelevantes/pagina/seguimientoasuntosrelevantespub.aspx?id=129659&seguimientoid=556*, última fecha de consulta el 29 de agosto de 2019.

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, Primera Sala. Novena Época. Semanario Judicial de la Federación y su Gaceta. Tomo XXVI, julio de 2007.

Tesis: 2a. LXIII/2008, Semanario Judicial de la Federación y su Gaceta, Novena Época, tomo XXVII, mayo de 2008, p. 229. [Las cursivas son propias], última fecha de consulta el 31 de octubre de 2019.

Tesis: P. II/2014 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, pleno, libro 3, febrero de 2014, tomo I.

Wikipedia, página oficial, disponible en: es.wikipedia.org/wiki/Ciclo_de _Deming, consultado el 12 de octubre de 2019.

Wikipedia, página oficial, disponible en *https://es.wikipedia.org/wiki/Internet_de_las_cosas#Definici%C3%B3n_original*, última fecha de consulta el 29 de agosto de 2019.

ZIEGELDORF, Jan Henrik, García Morchon, Oscar y Wehrle, Klaus, “Privacy in the Internet of Things: Threats and Challenges”, *Security and Communication Networks*, núm, 7, vol. 12, 2014, disponible en *https://arxiv.org/ftp/arxiv/papers/1505/1505.07683.pdf*, última fecha de consulta el 29 de agosto de 2019.