UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
POSGRADO EN CIENCIAS POLÍTICAS Y SOCIALES
FACULTAD DE CIENCIAS POLÍTICAS Y SOCIALES

Diseño Institucional y Organizacional de la Protección de Datos Personales en México

T E S I S

QUE PARA OPTAR POR EL GRADO DE
DOCTORA EN CIENCIAS POLÍTICAS Y SOCIALES

PRESENTA:
SOFIA SALGADO REMIGIO

TUTORA:
Dra. Cristina Puga Espinosa
POSGRADO EN CIENCIAS POLÍTICAS Y SOCIALES

Ciudad Universitaria, Cd. Mx. Abril, 2019

AGRADECIMIENTOS

A Cristina Puga,

Por su profesionalismo y humanidad.

Por ser la mejor tutora que pude tener.

Por su cariño y amistad.

A las mujeres que me formaron:

Sofía, Emilia, Leticia, Elisa, Araceli,

Cristina, Irma, Jacqueline y Gabriela.

En especial a Gabriela,

Por aparecer en mi vida y ser mi amiga;

la mejor guía e inspiración.

Con todo mi corazón para Irma,

Gracias por todo.

A mis amigas:

Verónica, Ana, Erika y Guadalupe.

A mis hermanas,

sus nombres los guardo siempre conmigo.

A todas las mujeres víctimas de la violencia en cualquiera de sus tipos.

INDICE

INTRODUCCIÓN

En la actualidad, el desarrollo tecnológico permite a los gobiernos y a las empresas recopilar grandes cantidades de información de las personas. La obtienen cuando se solicita un servicio, ejercen un derecho o cumplen una obligación. De esta manera, al realizar actividades cotidianas, como pagar impuestos, alquilar un video, utilizar la tarjeta de crédito, acudir al registro de votantes o al registro civil, realizar una llamada telefónica, adquirir un servicio o producto por medios electrónicos, mandar un correo o simplemente navegar en internet, los datos personales son registrados, almacenados y en muchos casos utilizados con fines distintos para lo cual fueron recabados.

La posesión de datos personales en el sector público y privado implica un problema cuando se desconocen o violentan los parámetros de recolección, uso, tratamiento y protección adecuados, de tal manera que se pone riesgo o afectan la privacidad e intimidad de la persona asociada a esos datos; perjudicando con esto su seguridad económica, jurídica, social e individual. “La negligencia y el uso lucrativo de esos datos ha implicado la venta, robo y pérdida de grandes bases de datos ocasionando fraudes económicos” (Piñar, 2008: 23), “robo de identidad, secuestros, hostigamiento, extorsiones y discriminación que afectan directamente a la persona propietaria de esos datos” (Ornelas, 2013). Un ejemplo cotidiano es el hostigamiento telefónico ¿cuántas veces te ha despertado un domingo por la mañana una llamada telefónica de un desconocido ofreciéndote un servicio?, situación de molestia a la que respondes con una pregunta ¿Y de dónde obtuvo mis datos para poderse comunicar conmigo? Esta y muchas otras vulneraciones suceden todos los días en México y en el mundo entero.

En este sentido, nos encontramos con un problema que nos obliga a reflexionar e investigar sobre la relación entre la persona, la tecnología, el gobierno, las empresas y el tratamiento de los datos personales. Un problema que nos afecta a todos, por lo que tenemos que iniciar el diálogo abierto, crítico y con razones que asistan tanto al individuo, a la comunidad y los intereses de terceros. De aquí que sea necesario conocer el origen del problema y las propuestas para resolverlo. En principio esta es la preocupación de la presente investigación, la cual brinda un panorama del diseño institucional y organizacional de la política para protección de datos personales en México

En el ámbito internacional, los esfuerzos por mostrar el panorama de este problema iniciaron en la década de los años sesenta con la Resolución 509 de la Asamblea del Consejo de Europa de

1968, la cual muestra un primer diagnóstico sobre cómo la vida de las personas se ve afectada por el desarrollo tecnológico, y la necesidad de la acción pública de los gobiernos en torno a este problema, el cual se agudizó a partir de los años ochenta con el desarrollo de la tecnología, los medios de comunicación y la computación, así como con el cambio del modelo económico —en la división internacional del trabajo, mediante encadenamientos globales de producción y la implementación de los esquemas administrativos modernos—, afectando la forma de interacción entre las personas, el gobierno y su entorno, por el uso de las tecnologías de la información y de la comunicación para hacer más eficientes tiempos, procesos y productos, facilitando con mayor agilidad el intercambio de datos y modificando las necesidades de la vida moderna con el uso cotidiano de las redes sociales, el correo electrónico, las computadoras y los teléfonos móviles, entre otros medios de interacción digital.

Sin duda estos cambios han traído beneficios, pero también han ocasionado daños. Por ejemplo, las empresas logran decisiones más eficientes a partir de la información obtenida por robots informáticos en las redes sociales. Este mismo caso es muestra de la vulnerabilidad de la persona en un contexto digital, así como de la incertidumbre que puede generar la cantidad de información presentada en estas plataformas, y por ello descuidar o restarle importancia a la recolección de sus datos personales por parte de estas empresas, como las redes sociales que obtienen grandes cantidades de datos personales y los patrones de conducta: gustos, preferencias, nivel educativo, edad, situación sentimental, ideologías y datos biométricos, sólo por mencionar algunos.

Ante estos hechos, es necesario preguntarse, cómo entender este problema, cómo darle solución; cuál es el papel de las personas, el gobierno y las empresas ante el tratamiento de los datos personales; cuáles son las necesidades y los acuerdos a los que debemos llegar en lo individual y colectivo. Las incógnitas no son menores y las repuestas, nada sencillas. Sin duda el problema es complejo e incorpora diversas aristas que deberán ser atendidas a la luz de su origen y de las alternativas disponibles (Lindblom, 1959). Estos son algunos motivos que justifican la selección del tema, por lo que esta investigación logra excelentes resultados para atender las preguntas aquí planeadas, desde un enfoque nacional e internacional.

En México el problema ha cobrado relevancia en los últimos años. En 2001 se presentó la primera iniciativa de ley sobre protección de datos personales; la primera regulación específica se dio en el ámbito público con la Ley de la Información Pública Gubernamental (11 de junio del 2002) y con los lineamientos de protección de datos personales de 2005. En 2009 se aprobó la ley

que regula el uso de datos por parte del sector privado, y finalmente en 2016 surge la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, la cual trata de estandarizar principios, procesos y la regulación a nivel nacional. Esta ley entró en vigor en enero del 2017.

Entonces, uno de los grandes problemas aquí planteado es el uso y protección de los datos personales, el cual ha sido muy poco estudiado, en este sentido es de suma importancia comprender su diseño y ejercicio, tanto en el sector público como en el privado. Es un problema que se incrementa ante la compleja relación entre los derechos fundamentales de las personas, el uso de las tecnologías por parte del Estado moderno (Fountain, 2013) y las necesidades económicas del entorno nacional e internacional. Como vemos, el asunto no es menor, porque la persona en lo individual se convierte en el centro de acción estatal (Uvalle, 2017).

La protección de los datos personales se reconoció en México como un derecho humano fundamental el primero de junio del 2009 en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, por lo tanto, es uno de los últimos derechos garantizados constitucionalmente en nuestro país. En la Unión Europea la regulación en materia de protección de datos personales fue impulsada por países como Alemania en 1970 y diversos organismos internacionales. Esto dio como origen nuevos procesos, procedimientos, lineamientos y sistemas informáticos, incluyendo nuevos servicios. El tratamiento de datos creó sistemas administrativos, jurídicos, informáticos y económicos complejos que nos obligan a profundizar en el conocimiento de este derecho humano, pues se ha convertido en un problema público que ha repuntado en las agendas internacional y nacional.

Por tales razones, en esta investigación se presenta el estudio de los motivos que influyeron en el diseño institucional y organizacional de la protección de datos personales en México: el origen del problema, la construcción de las normas, la elección de la autoridad garante, la definición de los procesos y procedimientos de protección, así como las fortalezas y las debilidades del diseño. Es decir, se analizan aspectos esenciales del problema que nos permitan llegar a soluciones adecuadas a nuestras necesidades y entorno.

Conocer cómo se diseñaron tanto las instituciones como las organizaciones para atender la política para la protección de los datos personales resultó relevante en la medida que permite entender cómo a partir de un problema público complejo —como lo es un derecho humano fundamental—, las decisiones tratan de conciliar amplios intereses económicos y políticos. En donde el contexto provee oportunidades o barreras al diseño institucional (Weimer, 2011).

Como parte de los resultados, se logró confirmar que el diseño institucional y organizacional de la política para la protección de datos personales en México fue producto de la negociación de diversos actores: autoridades administrativas del Estado, el sector empresarial, tanto nacional como internacional, y algunos miembros de la sociedad civil, principalmente representada por académicos y periodistas. Al incluir los intereses de estos sectores, se presentaron diversas opciones para atender el problema, eligiendo la solución que permitió mayor flexibilidad institucional y organizacional. Fue una decisión limitada (Lindblom, 1959) y fragmentada que priorizó ciertos valores, intereses y objetivos por encima de otros. Este diseño flexible y limitado resulta insuficiente para resolver el problema por su falta de robustez, integridad y sistematicidad pues el diseño atendió más el argumento de las coaliciones de actores más organizados, dejando espacios de vulnerabilidad institucional para las personas carentes de organización y herramientas de defensa sistémica.

En suma, el diseño institucional y organizacional de la protección de datos personales debilita las estructuras del Estado; limita sus responsabilidades, su función administrativa y su control en el manejo de los asuntos públicos; disminuye las responsabilidades gubernamentales y las distribuye a otros actores públicos y privados, dejando espacios de incertidumbre legal y organizacional donde el control y protección de los datos es más difícil y, por lo tanto, deja en alto grado de incertidumbre y vulneración la seguridad y la privacidad de los ciudadanos.

Para llegar a estos hallazgos, el proceso metodológico constó de cuatro etapas. En la primera se utilizaron herramientas de la metodología cualitativa. El estudio partió de la revisión bibliográfica exhaustiva nacional e internacional, continuó con el análisis de contenido de las resoluciones jurídicas de organismos internacionales; convenios internacionales; leyes nacionales; reglamentos, lineamientos y otras disposiciones aplicables al caso mexicano.

En la segunda etapa se realizó trabajo de archivo en el Congreso de la Unión para conocer y mapear el proceso legislativo relacionado con las iniciativas presentadas y su dictamen, donde se logró identificar quiénes participaron en las propuestas de ley y las autoridades afines al tema como el IFAI (ahora INAI)[1], la Secretaría de Economía (SE), la Procuraduría Federal del Consumidor (PROFECO), entre otras instituciones interesadas.

En un tercer momento, la estrategia metodológica consistió en realizar entrevistas con

[1] La Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) de 2015 cambia el nombre del Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) a Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), a partir del 16 de mayo del 2015.

actores que participaron tanto en el diseño como en el rediseño para definir las instituciones —reglas formales— y las organizaciones —autoridades— en materia de protección de datos personales. Del conjunto de estos actores se realizaron entrevistas con funcionarios y exfuncionarios del INAI y de la Secretaría de Economía; expertos internacionales y nacionales, representantes del sector privado y diputados implicados en las iniciativas de ley.

Finalmente, se puso a prueba este diseño institucional para conocer sus fortalezas y debilidades mediante el estudio de caso. Se decidió analizar la *e-firma* del Servicio de Administración Tributaria (SAT) por tres razones: corresponde a un asunto público; se ven implicados el sector gubernamental, el empresarial y el social en el proceso de trámite, uso y tratamiento de los datos personales. Además, es una de las bases de datos gubernamentales que tiene información biométrica considerada como altamente sensible, como el iris de ambos ojos y las diez huellas dactilares. Sin duda, los casos dignos de análisis son muchos y ahora han aumentado, sin embargo, dado el origen de la investigación, sus objetivos y el enfoque, fue el caso viable que se decidió analizar.

La tesis se divide en cuatro capítulos. En el primero se definen los principales conceptos que permiten comprender los apartados de esta investigación, desde el punto de vista teórico conceptual: Estado, persona y dato personal. Dado que esta investigación es sobre el diseño institucional y organizacional, el enfoque teórico que se utiliza es el nuevo institucionalismo, a partir del cual se entrelaza el tema de los derechos humanos y el enfoque sobre el diseño de las políticas públicas.

En el segundo capítulo se presenta el resultado analítico de la historia sobre la protección de datos personales a nivel internacional. Es el apartado donde se muestran los problemas públicos que se tratan de resolver en los dos modelos dominantes: el de la Comunidad Europea (CE) y el de los Estados Unidos de América (EUA). El primero más garantista de un derecho humano fundamental, que pone límites a herramientas digitales y/o físicas en el manejo, tratamiento o transferencia de los datos personales. El segundo, el de los EUA, más sectorial y concentrado en un conjunto amplio y complejo de medidas de autorregulación tanto para el sector público como para el privado, donde la descentralización de las normas motiva la mínima regulación del sector económico. Aquí la regulación y el control dependen del tipo de dato personal y del sector económico que trata estos datos.

El diseño institucional y el organizacional de la protección de datos personales en México es analizado en el tercer capítulo. Se ofrece el análisis desde la primera iniciativa de ley presentada

en 2001 hasta la propuesta de Ley General de Protección de Datos Personales que entró en vigor en enero de 2017; a su vez se encontrarán las diversas propuestas de diseño organizacional ideado para fungir como el órgano garante de la protección de datos personales y cómo el IFAI (ahora INAI) fue el órgano elegido. Este análisis es teórico, histórico y empírico. Se fundamenta en la revisión de documentos formales, pero también en un conjunto amplio de entrevistas realizadas con los actores involucrados en el diseño: Alfredo Reyes Kraft, Edgardo Martínez, Gustavo Parra Noriega, Jacobo Esquenazi, María Marván Laborde, Issa Luna Pla, José Luis Piñar Mañas y Miguel Recio Gayo. Con las aportaciones de los entrevistados se identificaron las principales características del diseño de protección de datos personales en México: sus objetivos, principios y actores involucrados en la negociación de esta política. El resultado fue un diseño de política regulativa para la protección de datos personales en México.

Este diseño se pone a prueba en un cuarto capítulo, donde se analiza el uso y tratamiento de datos personales en la *e.firma* del SAT. En este caso, se analizan los límites del diseño, concentrándose en las institucionales y organizacionales encontradas en torno a la protección de datos personales tratadas en esta institución pública gubernamental. Finalmente, en el quinto capítulo se comparte un análisis mucho más amplio, donde se narran las repercusiones del modelo de protección de datos personales para tres actores implicados en su diseño: personas, gobierno y empresas, lo que permite concluir con algunas reflexiones finales, comentarios a los avances actuales del diseño, las propuestas y líneas de investigación futuras.

En resumen, en esta investigación se analizó el diseño de la política para la protección de datos personales en México, partiendo del enfoque institucional liberal, democrático y de derecho como centro de la regulación y protección de los derechos humanos, y las necesidades económicas nacionales, tratando de equilibrar y reconocer las consecuencias en la toma de decisiones políticas y económicas en torno a un derecho humano fundamental, en un contexto de amplia complejidad como el mexicano. Con un sistema económico mixto que reconoce la necesidad de promover la competencia económica, pero que también se fundamenta en principios y valores nacionales como el respeto a los derechos humanos fundamentales y a la dignidad de las personas.

CAPÍTULO 1. LA REGULACIÓN DE LOS DATOS PERSONALES

"Los derechos importan, porque nunca sabes cuándo vas a necesitarlos"
(Snowden, 2014)

El Estado es la máxima institución creada para regular el comportamiento social. Para lograr su objetivo se apoya en sistemas normativos y administrativos, cuyo diseño depende de diversos factores. En el presente capítulo se muestra el entramado teórico conceptual que nos permite entender cuáles son los diferentes motivos y circunstancias que dan origen a las instituciones y a las organizaciones púbicas. Este apartado analítico es importante en la medida que muestra cómo se regula un derecho humano fundamental a partir de una política regulativa por parte del Estado y otros actores, modificando el comportamiento social. Nos muestra cuál es el papel del Estado frente a este derecho y cuáles son las alternativas para diseñar tanto las instituciones como las organizaciones encargadas de velar por un derecho: la protección de datos personales.

1.1 Los datos personales

De acuerdo con la Real Academia de la Lengua Española (RAE, 2016) "dato" proviene del latín *datum* que significa "lo que se da" y adquiere sentido cuando el concepto se profundiza al definirlo como "información sobre algo concreto que permite su conocimiento exacto" o como "la información dispuesta de manera adecuada para su tratamiento por una computadora". Estas definiciones de la RAE permiten identificar algunos aspectos del concepto de los cuales podemos entender que el dato surge a partir de un sujeto, objeto o agente. Es decir, se requiere un agente que posee información de sí mismo, y que puede desprenderse de esos datos, los cuales se convierten en información que identifica al propio agente. Si esto lo trasladamos a una persona, el punto de partida es que ésta posee atributos que en sí mismos son datos que proveen información sobre y de sí misma.

Estos datos son inherentes a la persona, pero pueden desprenderse de está y ser dados (no cedidos) para diferentes fines. Antes de continuar es importante definir lo que se entiende por persona. El término persona tiene por lo menos dos acepciones: la moderna y la antigua: la primera relaciona el concepto con el ser humano, y la antigua con una ficción creada y definida a partir de ciertos atributos (Huber, 2007: 535). Esta última acepción está relacionada con los sujetos de

derecho de goce y disfrute. Aquí lo importante es dejar claro que cuando hablamos de persona nos referimos a un sujeto de derecho que es un ser humano, el cual tiene derechos y obligaciones. Si dejamos esto como premisa consideramos que incluso cuando se habla de personas colectivas y éstas hagan referencia a un ser humano, entonces se entiende como persona para los fines de esta investigación. Y si una persona colectiva no hace referencia a una persona humana simplemente quedará fuera de la categoría aquí estudiada.[2]

Una vez realizada la definición de dato y persona, es necesario definir qué entendemos por dato personal. Las legislaciones internacionales en la materia coinciden en que es "toda información sobre una persona física identificada o identificable" (OCDE, 1980; CE, 1981; PE y CE, 1995; APEC, 1998 y AGPD, 2009) y aunque también la mayoría de las leyes incluyen tal definición, hay casos como el de Canadá que hacen especificidades, como las siguientes, en que los datos personales son:

> "Toda la información sobre una persona física que la identifica o la hace identificable y que sin limitar la generalidad de tal definición, puede considerar la siguiente información: "la relativa a la raza, origen nacional o étnico, color, religión, edad o estado civil; la información relativa a la educación o la historia médica, penal o laboral de la persona; las transacciones financieras en las que se ha involucrado una persona; cualquier número de identificación o símbolo particular que se le asigne al individuo; la dirección, las huellas digitales o el tipo de sangre de la persona; las opiniones personales o puntos de vista del individuo; la correspondencia enviada a una institución gubernamental para un individuo con carácter implícito o explícito de privado y confidencial y la respuesta a esa correspondencia" (*Privacy Act*, 2011:3).

Esta definición demuestra la amplia concepción que puede adquirir los datos de una persona "en diversos contextos de regulación" (Bennett, 2003: 163-185). Es decir, dado que no existe un catálogo único sobre los datos personales, la diversidad a la hora de definirlos suele ser una categoría necesaria de considerar.

Para el reglamento del Parlamento Europeo y del Consejo (2016, Art. 26) los datos

[2] Esta categoría conceptual de persona es importante en la medida que permite considerar que las personas colectivas, es decir las morales, tienen derecho a la protección de los datos personales. Por ejemplo, cuando los datos sean de una persona moral, pero recaigan en un individuo, entonces se consideran datos personales. Para profundizar en este tema puede consultarse: SCJN, 2014. "Personas morales. Tiene derecho a la protección de los datos que puedan equipararse a las personas, aun cuando dicha información haya sido entregada a una autoridad." Gaceta del Seminario Judicial de la Federación. Pleno. Decima Época. Libro 3, febrero de 2014, página 274.

personales pueden determinar la identidad de manera directa o indirecta, "mediante un número de identificación; uno o varios elementos específicos, característicos de su identidad física, fisiológica, genética, psíquica, económica, cultural o social". En el caso mexicano la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados (LGDPDPPP) contempla los siguientes conceptos:

a) "Por dato personal se entiende 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;
b) Por datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual" (LGPDPPP, 2017: 1),

Como se puede observar, estas definiciones refieren cuatro características importantes: datos que al unificarse revelan información de una persona: la determinación de la identidad de manera directa o indirecta; los tipos de datos personales, y los tipos de daños que puede ocasionar su tratamiento. Estas categorías nos permiten definir dato personal como todo atributo que integra a una persona en su totalidad y mediante el cual se puede identificar o hacer identificable de manera directa o indirecta, por cualquier medio, tiempo y espacio. De tal manera que los datos personales (en plural) serán toda aquella información que se derive del dato personal en su unidad y pluralidad para identificar o hacer identificable a una persona, pudiéndole ocasionar daños y perjuicios en la vida posesión e integridad física y mental.

En el siguiente cuadro se presenta una primera clasificación sobre los datos personales que podemos encontrar como atributos de una persona. No es una lista exhaustiva, pero si logra sistematizar y definir diversos tipos de datos personales.

Cuadro 1. Clasificación de los datos personales.

Datos médicos	Datos laborales	Datos de identidad	Datos ideológicos

- Discapacidades
- Intervenciones quirúrgicas
- Vacunas
- Consumo de medicamentos
- Uso de aparatos oftalmológicos, ortopédicos, auditivos, entre otros (anteojos, aparatos de oído, prótesis, etc.)
- Estado de salud
- Historial clínico
- Alergias
- Enfermedades crónicas degenerativas
- Incapacidades médicas
- Enfermedades familiares
	- Documentos de reclutamiento y selección
	- Nombramientos
	- Teléfono institucional*
	- Actividades extracurriculares
	- Referencias laborales
	- Referencias personales (cartas de recomendación, etc.)
	- Trabajo actual
	- Trabajos anteriores
	- Documentos de capacitación
	- Puesto / cargo*
	- Domicilio de trabajo*
	- Correo electrónico institucional*
	- Exámenes psicométricos
	*Aplica para el sector privado.
		- Nombre
		- Apellidos
		- Nacionalidad
		- Lugar de nacimiento
		- Fecha de nacimiento
		- Edad
		- Fotografía
		- Domicilio
		- Teléfono del domicilio
		- Teléfono celular particular
		- Correo electrónico
		- Estado civil
		- Firma
		- Firma electrónica
		- Costumbres
		- Idioma
		- RFC
		- CURP
		- Cartilla militar
			- Creencias
			- Religión
			- Ideas,
			- Ideales,
			- Ideología (s)
			- Afiliaciones
			  - Política
			  - Sindical
			  - Religiosa
			  - Social
			  - Económica
			  - Filosóficas
			- Afinidades
			  - Dogmáticas
			  - Doctrinales
			  - Paradigmáticas
			  - Teóricas
			- Pensamientos
			- Opiniones

Datos patrimoniales	**Datos jurídicos**	**Datos migratorios**	**Datos académicos**
- Afores - Fianzas - Servicios contratados. - Referencias personales, crediticias o patrimoniales - Bienes muebles e inmuebles - Información Fiscal. - Historial crediticio - Ingresos y egresos - Cuentas bancarias - Seguros diversos	- Procesos judiciales, - Procedimientos judiciales en diversas materias - Resoluciones judiciales - Edictos, - Solicitudes judiciales - Demandas de la esfera jurídica de una persona, - Juicios - Sentencias	- Número de pasaporte - Número de visa (s) - Lugares visitados - Países visitados - Solicitudes de asilo, - Viajes, - Motivos de viajes, - Información relativa al tránsito de las personas dentro y fuera del país - Información migratoria de las personas	- Estudios realizados, - Escuelas a las que asiste o asististe - Modelos académicos de formación, - Trayectoria educativa - Títulos - Cédula profesional - Certificados - Reconocimientos - Desempeño Académico - Calificaciones - Examenes
Datos físicos	**Datos biométricos**	**Datos sexuales**	**Datos protoeonómicos / químicos**
- Características del cuerpo, piel, iris, cabello, entre otros: - Longitud, - Estatura - Peso - Complexión - Tatuajes - Otras características relacionadas al aspecto físico	- Iris ocular / retina - Secuencia genética (ADN) - Tipo de sangre - Huella (s) dactilares, facial, manos, venas, pies, dentales, bucales (voz) - Geometría de la mano - Reconocimiento facial - Oreja biométrica - Firma	- Género - Preferencias - Hábitos - Número de parejas, - Inicio de actividad sexual	- Secuencias proteínicas de especie - Rutas metabólicas de las células, - Olor - Marcadores hormonales, - Estudios químicos, - Medición de elementos

Datos alimenticios	Datos familiares	Datos culturales	Datos psicológicos
- Tipo de alimentación - Preferencias en alimentación - Horas de alimentación - Tipo de bebidas - Hábitos alimenticios - Desórdenes alimenticios	- Número de hijos - Nombre de padre y madre - Número de hermanos - Nombres de hermanos y hermanas. - Otros parentescos - Ascendencia - Descendencia	- Región de origen - Cultura de origen - Cultura adscrita - Tradiciones - Costumbres - Idioma (s) - Lengua nativa - Origen racial - Origen étnico	- Información relacionada con cuestiones de carácter psicológico y/o psiquiátrico - Fobias - Estados anímicos - Construcciones mentales
Pasatiempos	**Hábitos comerciales**	**Habilidades**	**Otros datos**
- Lugares de diversión cotidiana, - Gustos culturales - Música - Baile - Literatura, - Teatro - Música - Videojuegos - Gustos por la literatura - Gustos por el cine	- Fracturas - Gustos - Preferencias comerciales. - Marcas de preferencia - Lugares cotidianos de compras	- Toma de decisiones - Deportes - Juegos - Destrezas - Actos extraordinarios que lo diferencia de la generalidad - Dibujo, Arte, Cine, Fotografía - Utilizar herramientas o tecnología específicas. - Programaciones y lenguajes.	- Número de teléfono celular particular. - IP del computador. - Conversaciones privadas e íntimas en redes sociales o de la comunicación. - Contraseñas personales diversas

Fuente: Elaboración propia con base en el sistema persona del IFAI (2012) y diversas legislaciones internacionales.

El cuadro anterior no es exhaustivo, de allí que sea sólo una primera propuesta de clasificación, misma que incorpora una lista amplia de datos, pero reconoce la generalidad de los atributos (no sólo jurídicos) de una persona en su integridad por lo que no es limitativa. A partir de esta primera definición y clasificación tanto de dato personal como de los datos personales podemos profundizar sobre cómo es que esta información adquiere la importancia de ser protegida y los parámetros a partir de los cuales podemos entenderla.

1.2 El derecho a la protección de datos personales

Hoy la protección de datos personales en un derecho humano fundamental autónomo de tercera generación. Si bien tiene parte de su fundamento en valores y principios de los derechos de primera generación como la libertad y la libertad de información, adquiere mayor relevancia en el contexto que se caracteriza por regímenes políticos más o menos democráticos, economías de libre mercado, procesos administrativos digitales, uso de herramientas computacionales y el

desarrollo de las tecnologías de la información y la comunicación.

La protección de datos personales tiene un vínculo estrecho con el derecho a la libertad, específicamente el derecho a la libertad de expresión, el derecho a la autodeterminación informativa, el derecho a la privacidad, el derecho a la intimidad y el derecho de acceso a la información pública. Aquí es necesario detenerse para analizar estas relaciones, las cuales nos permitirán definir y conocer el proceso a través del cual la protección de datos personales se convierte en un derecho con fines y objetivos propios.

La libertad como concepto ha sido materia de profundos estudios con diversos enfoques. La libertad cobra sentido cuando es reconocida a todos por igual y bajo las mismas condiciones; obviamente el reconocimiento de la libertad en condiciones de igualdad no genera, por sí mismo y de forma automática un igual ejercicio de la libertad por cada persona (Carbonell, 2004: 302). La mayor parte de los análisis teóricos están de acuerdo en distinguir dos formas de libertad: la negativa y la positiva. Esta distinción conceptual parte de las ideas de Benjamin Constant en 1819, en su ensayo de la libertad de los antiguos comparada con la de los modernos. Para Constant la libertad de los antiguos consistía:

> "En ejercer la forma colectiva pero directa, diversos aspectos del conjunto de la soberanía, en deliberar en la plaza pública sobre la guerra y la paz. En concluir alianzas con los extranjeros, en votar las leyes, en pronunciar sentencias, examinar las cuentas, los actos, la gestión de los magistrados; en hacerlos comparecer ante todo el pueblo, acusarles, condenarles o absolverles; pero a la vez que los antiguos llamaban libertad a todo esto, admitían como compatible con esta libertad colectiva la completa sumisión del individuo a la autoridad del conjunto. Todas las actividades privadas estaban sometidas a una severa vigilancia; nada se dejaba a la independencia individual, ni en relación con las opiniones, ni con la industria ni, sobre todo, con la religión" (Constant, 1989 [1819], 260).

En comparación, la libertad de los modernos la definía como:

> "El derecho de cada uno a no estar sometido más que a las leyes, a no poder ser ni arrestado, ni detenido, ni muerto, ni maltratado de manera alguna a causa de las voluntades arbitrarias de uno o varios individuos. Es el derecho de cada uno a expresar su opinión, a escoger su trabajo y a ejercerlo, a disponer de su propia vida, y abusar incluso de ella; a ir y venir sin pedir permiso y sin rendir cuenta de sus motivos o de sus pasos. Es el derecho de cada uno a reunirse con otras personas, sea para hablar de sus

> intereses, sea para profesar el culto que él y sus asociados prefieran, sea simplemente para llenar sus días y sus horas de manera más conforme a sus inclinaciones, a sus caprichos. Es, en fin, el derecho de cada uno a influir en la administración del gobierno, bien por medio del nombramiento de todos o de determinados funcionarios, a través de representaciones, de peticiones, de demandas que la autoridad está más o menos obligada a tomar en consideración" (Constant, 1989 [1819]: 259 y 260).

De esta manera, para Constant la libertad ha cambiado. Antes se ejercía la liberad a partir de los actos públicos y de la relación con otros. Ahora, en la modernidad, la libertad alude al ejercicio individual. Isaiah Berlin retoma la idea de la libertad para los modernos a mediados del siglo XX, haciendo alusión al problema de la obediencia y de la coacción, tratando de responder a las preguntas: "¿Por qué debo yo (o cualquiera) obedecer a otra persona?, ¿por qué no vivir como quiera?, ¿tengo que obedecer? Si no obedezco, ¿puedo ser coaccionado? ¿Por quién, hasta qué punto, en nombre de qué y con motivo de qué?" (Berlin, 1819: 2). Es decir, se cuestiona los límites que pueden permitirse a la coacción individual, diferenciando entre libertad negativa y positiva.

Estas libertades nos permiten aclarar y profundizar por qué la libertad es uno de los antecedentes más importantes para entender el derecho de la protección de datos personales, pues ambas se fundamentan en el ejercicio de la libertad de la persona a partir de la acción individual de ser y hacer en dos tipos de espacios: el público y el privado.

> El primero de estos sentidos el "*negativo*, es el que está implicado en la respuesta que contesta a la pregunta *cuál es el ámbito en que al sujeto —una persona o un grupo de personas— se le deja o se le debe dejar hacer o ser lo que es capaz de hacer o ser, sin que en ello interfieran otras personas*. El segundo sentido, el *positivo*, es el que está implicado en la respuesta que contesta a la pregunta de *qué o quién es la causa de control o interferencia que puede determinar que alguien haga o sea una cosa u otra*. Estas dos cuestiones son claramente diferentes incluso aunque las soluciones que se den a ellas puedan mezclarse mutuamente (Berlin, 1819: 2).

Así, las respuestas para el sentido negativo de la libertad y el sentido positivo son en origen a partir de los espacios para el ser y el hacer de la acción humana. Retomando la idea de Isaíah Berlin (1819) "ser libre (en el sentido negativo) quiere decir que otros no se interpongan en la actividad individual de la persona y cuanto más extenso sea el ámbito de esta ausencia de interposición, más

amplia será la libertad." En esta libertad negativa se reconoce la imposición de restricciones a la libertad, pero también se pretende que sean las menos, con el objetivo de que el ámbito de la libertad sea superior. Es una libertad con interferencia que tiene un límite, mismo que es intercambiable pero siempre posible de identificar.

Este tipo de libertad tiene dos aspectos importantes. El primero es reconocer que "la libertad no es ni la primera necesidad de todo el mundo, ni el único fin del hombre". Esto es sumamente importante porque si partimos de este supuesto estaríamos aceptando que la libertad tiene límites y esos límites aparecen cuando reconocemos que la libertad desde un aspecto político incluye la interacción con otros que tienen necesidades diferentes. Entonces se puede ceder o sacrificar libertad para buscar igualdad, felicidad, cultura o seguridad, por poner algunos ejemplos. Al mismo tiempo, esta libertad negativa está reconociendo:

> "[…] que debía existir un cierto ámbito mínimo de libertad personal que no podía ser velado bajo ningún concepto, pues si tal ámbito se traspasaba, el individuo mismo se encontraría en una situación demasiado restringida, incluso para ese mínimo desarrollo de sus facultades naturales, que es lo único que hace posible perseguir, e incluso concebir, los diversos fines que los hombres consideran buenos, justos o sagrados. De aquí se sigue que hay que trazar una frontera entre el ámbito de la vida privada y de la autoridad pública", tal como lo manifestaron Locke, John Stuart Mill, Benjamín Constant y Tocqueville" (Berlin, 1819: 4).

Entonces la libertad en sentido negativo es la que tiene el individuo en relación con ciertas restricciones, que tienen un límite y reconocen la necesidad de no interferir en un determinado espacio del individuo. "No podemos ser absolutamente libres y debemos ceder algo de nuestra libertad para preservar el resto de ella" (Berlin, 1819: 6). De esta manera, al mismo tiempo que existen normas que limitan esa libertad en busca de proveer otros fines como la seguridad, la felicidad, la igualdad e incluso la provisión de mejores oportunidades de desarrollo económico, se reconoce un espacio para la persona (ser humano) libre de intervención que le permita ser y hacer. Este punto será sumamente importante para nuestra discusión sobre la protección de datos personales en torno al diseño de sus estructuras institucionales y organizacionales.

El otro aspecto de la libertad es el positivo, el cual "consiste en ser dueño de sí mismo" (Berlin, 1819) y responde a la pregunta ¿Quién tiene que decir lo que yo tengo y lo que no tengo que ser o hacer? Aquí el individuo reconoce que tiene la necesidad de mantener su propia

identidad, tal como se manifiesta de la siguiente manera:

> "[…] Quiero que mi vida y mis decisiones dependan de mí mismo; ser instrumento de mí mismo y no de los actos de voluntad de otros hombres. Quiero ser sujeto, no objeto, ser movido por razones y propósitos míos y no por causas que me afecten. Tengo el deseo de ser alguien y no nadie; actuar, decidir y no que decidan por mí; dirigirme a mí mismo y no ser movido por la naturaleza exterior o por otros hombres como si fuera una cosa. Ser consciente de mí mismo como ser activo que piensa y que quiere, que tiene responsabilidad de sus propias decisiones y que es capaz de explicarlas en función de sus propias ideas y propósitos. Yo me siento libre en la medida en que creo que esto es verdad y me siento esclavizado en la medida en que me hacen darme cuenta de que no lo es" (Berlin, 1819: 9).

Entonces, con la libertad positiva se logra evidenciar la necesidad de la propia identidad e imagen del individuo como ser humano. Por lo tanto, las aportaciones tanto de Benjamín Constant como de Isaíah Berlin permiten decir que el Estado moderno liberal fue constituido y pensado a partir de la libertad individual en términos modernos, y esto implica que el Estado reconozca un espacio de no intervención. Este concepto de "libertad de los modernos" no sólo permite hacer esta aseveración, sino también sienta las bases para que Isaíah Berlin construya el concepto de libertad negativa.[3] El cual nos permite entender la imposición de normas a la acción individual, pero sólo como un medio para conseguir la independencia. Y la libertad positiva permite entender la voluntad que tienen los individuos sobre sus acciones, así como la autonomía de las mismas y de su propia voluntad. Entonces libertad negativa "equivale a la no interferencia, a la posibilidad de actuar sin que nadie se interponga u obstaculice los actos; es un espacio exento de coacción. Es decir, en la medida que una persona realice actividades privadas no debe ser importunado en modo alguno" (Carbonell, 2004: 49)

Así, mientras la libertad negativa está relacionada con la esfera de las acciones, la positiva se relaciona con la esfera de la voluntad. Ambas libertades coinciden con la idea de que el individuo tiene un grado de acción y voluntad para actuar en un contexto social determinado. Este

[3] Conviene señalar que la calificación de negativa y positiva que se aplica al término libertad no tiene un significado axiológico, sino simplemente lógico, es decir, no es que el primer tipo de libertad sea indeseablemente perjudicial y el segundo deseable y benéfico, sino que se denomina de esa forma por la virtud de su contenido. Para profundizar, véase: Berlín, Isaíah. *Dos conceptos de libertad*. 1958. Universidad de Oxford. Además: Carbonell, Miguel. 2004. *Los derechos fundamentales en México. México*. Comisión Federal de los Derechos Humanos e Instituto de Investigaciones Jurídicas, UNAM.

grado de acción y voluntad se relacionan con capacidades para actuar o no, mediante la no interferencia en un ámbito exclusivo de libertad y la posibilidad de ser del propio individuo.

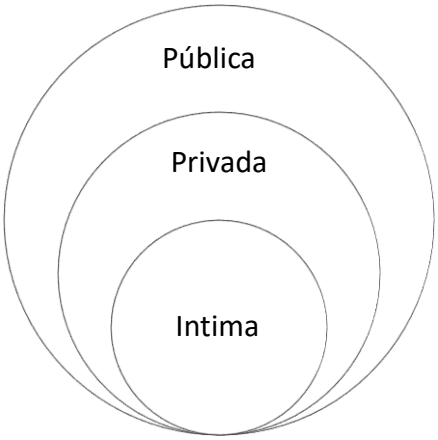
Ahora bien, ambas libertades muestran una contención entre derechos. Por un lado, el derecho a ser y hacer según ellos mismos y, por otro lado, el derecho de otros que originan la imposición de ciertas restricciones al ser y hacer del individuo. Por ejemplo, se dice que para ejercer el derecho a la libre expresión es necesario estar provisto de información (Dahl, 1971). De esta manera se reconoce la necesidad de tener acceso a la información como parte de la libertad de expresión, la cual se ve restringida por las afectaciones a terceros, como el daño moral, la dignidad de terceros; la seguridad nacional, la seguridad pública; el interés general; la intimidad y la privacidad de las personas.

Justo aquí se encuentran otros conceptos (que también son derechos antiguamente constituidos) importantes para esta investigación: privacidad e intimidad, que no pueden ser utilizados como sinónimos. Ambos se constituyen como derechos que protegen un ámbito de vida fuera de la autoridad del Estado o de la intromisión de un tercero, pero en niveles diferentes.

Para comprender privacidad e intimidad es necesario remitirse a dos conceptos importantes: lo público y lo privado. “Para los griegos la distinción entre lo público y lo privado permaneció sólida y nunca se puso en duda, la primera estaba delimitada por la esfera doméstica y la segunda por la vida política. Con el auge de la vida doméstica a la luz de la esfera pública, se borró la línea fronteriza entre lo privado y lo político” (Arendt, [1958] 2007: 49). Las categorías de bienes públicos o privados posibilitan la diferenciación de cada esfera. Los bienes colectivos corresponden a la esfera de lo público y los bienes privados a la privada (Arendt, [1958] 2007), esto nos permitirá dirimir controversias al momento de interactuar en una situación que contraponga derechos, pues a partir de definir si se trata de bienes públicos o de bienes privados se diferencian esferas y con ellos el derecho que se sobreponga al otro.

La relación entre las esferas pública, privada e íntima se puede ver el siguiente esquema.

Esquema 1. Las esferas pública, privada e íntima



Fuente. Elaboración propia

La vida de una persona se desenvuelve en diferentes esferas. En la pública se convive con otros compartiendo bienes de interés colectivo. En la privada, la información personal permanece a la vista de pocos, de la familia o amistades cercanas. Es la posibilidad de poner límites a otros sobre el ser y hacer cotidiano de las personas; tener la posibilidad de aislarse en la soledad, en el anonimato, la confidencialidad, la autonomía y la reserva de su vida. Por su parte, el espacio de la vida íntima está más alejado de la esfera pública, de allí que la información contenida en ese ámbito sea de origen más delicado en su trato.[4] El derecho a la intimidad protege la parte que define la identidad individual de una persona; es la esfera que sólo se reconoce en la profundidad de los pensamientos y la psique del propio individuo.

En su sentido original, el derecho a la intimidad se asocia con la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario para mantener la identidad individual. "El derecho a la intimidad abarca aquello que se considera más propio y oculto del ser humano –entendiéndose por propio y oculto la información que mantiene para sí mismo– (García, 2005: 94 – 110). La intimidad es un aspecto individualista, que se destina a salvaguardar un espacio que contiene la identidad más profunda del ser.

Hablar de intimidad es hablar de sentimientos, pensamientos y creencias; de información genética, por ejemplo. "Se trata de aquellos datos que bajo pocas circunstancias proporciona un

[4] Para profundizar, consultar García González, Aristeo. 2005. *Derecho a la intimidad desde una perspectiva constitucional: equilibrio, alcance, límites y mecanismos de defensa*. México, Universidad Michoacana de San Nicolás de Hidalgo. También véase: Farinas Matoni, Luis María. 1983. *El derecho a la intimidad*. Madrid, Trivium.

individuo. De aquí nacen, por ejemplo, los derechos a la inviolabilidad de las comunicaciones o el derecho a la propia imagen; ambos muy relacionados con la parte más íntima del individuo. Como tal es un derecho reconocido en el constitucionalismo internacional. Los términos y alcances del derecho no son fáciles de determinar, pues dependen de las condiciones culturales de la sociedad y de los medios jurídicos y democráticos que tengan tribunales y jueces en casos concretos" (Carbonell, 2004: 449).

En cada esfera se resguarda un derecho que se interrelaciona con los otros. Esta relación, parafraseando a Zygmunt Bauman (2010: 9) se puede materializar en "los campos semánticos de los conceptos, los cuales permiten un tráfico cruzado originando que el límite sea redundante, y dejando la posibilidad de que otros, quienes tienen el control y las herramientas del derecho puedan decidir a quién o qué se le permite pasar de un límite a otro". Esta discusión entre interés público y derechos individuales, entre comunitarismo y liberalismo es la paradoja entre estos derechos. Discutirlos aquí no es objetivo de este trabajo, pero sí nos permite brindar un panorama de las vertientes del problema.[5]

Otro de los derechos que guarda relación directa con la protección de datos personales es la autodeterminación informativa, derecho que "se basa en la decisión personal de preservar la identidad a través de la información propia que pudiera ser utilizada de forma incontrolada por terceros" (Piñar, 2006: 21). "Su esencia es el rechazo a cualquier intromisión en la vida privada del sujeto; otorga a su titular una posición jurídica de contenido positivo que se conforma sobre un haz de facultades destinadas a controlar el uso de información personal, tanto en el momento inicial de la recolección de datos, como en las fases posteriores de su tratamiento" (Del Castillo, 2007: 199). En este sentido, la autodeterminación informativa se vuelve el antecedente más próximo del derecho a la protección de datos personales, el cual le va a proveer a este último de elementos que definirán su contenido y fundamento.

El derecho a la autodeterminación informativa es reciente. Surge en la década de 1970 en Alemania y adquiere autonomía respecto a otros derechos de origen angloamericano, por ejemplo, con el derecho a la vida privada (*right to privacy*) y a la intimidad. Es definido como "el derecho a comunicar información personal con previo consentimiento" (Adinolfi, 2007: 21). Es aceptar el tratamiento de datos personales, siempre con la posibilidad de controlar su uso, circulación y

[5] Para profundizar sobre la visión comunitarista de la privacidad recomiendo revisar la obra de Etzioni, Amitai. 2012. *Los límites de la privacidad*. Actualidad criminológica y penal. Editorial, IB de F, Buenos Aires. También, Etzioni, Amitai. 2005. *How Patriotic is the Patriot Act?* Freedom Versus Security in the Age of Terrorism. New York. Routledge.

transmisión.

Actualmente, los derechos que implican la protección de un ámbito de la vida humana fuera de los alcances de un tercero (público o privado) han alcanzado senderos que hace algunos años no se habían contemplado. El derecho a la protección de datos personales recoge parte de la esencia de cada derecho antes mencionado; lo introduce como parte de su génesis, contenido y fundamento, pero se desvincula también al constituirse como un derecho autónomo. Se ha llegado a confundir la protección de datos personales con la privacidad, con la intimidad o con otros derechos, pero hoy cada uno tiene su propio contenido, reconocimiento y autonomía. Aunque esto no implica que entre ambos existan vínculos inseparables.

La protección de datos personales es un derecho de tercera generación que surge de manera autónoma en un contexto donde ha tenido auge el desarrollo de las tecnologías de la información y la comunicación. Es un derecho que puede entenderse de dos maneras: como un derecho intermediario. Es decir, "al ejercerlo se protegen otros derechos, como la privacidad, la intimidad o la libertad. También puede ser considerado como un derecho directo personalísimo, cuando la información personal no debe utilizarse para otros fines diferentes para los cuales se proporcionó a un tercero. Aquí se protegen los datos personales por sí mismos" (Ornelas, 2013).

Este derecho surge por la necesidad de reconocer la tutela de los datos a las propias personas, así como para regular el tratamiento de éstos por un tercero (público o privado). Como derecho fundamental se acepta su universalidad,[6] por ello fue necesario que se admitiera en contextos jurídicos y sociales diversos. Esta universalidad no supone uniformidad, pues "el contenido concreto depende de numerosos factores extrajurídicos, especialmente de la idiosincrasia, la cultura y la historia de los pueblos" (Konrad, 1996: 85). La teoría clásica de los derechos humanos consideraba que sólo el Estado podía vulnerar los derechos de las personas (Carbonell, 2004), pero con la evolución de la vida social se ha comprobado que los derechos también pueden ser vulnerados por privados, por ello la necesidad de reconocer este derecho y sus

[6] "La universalidad es un principio de los derechos fundamentales, la cual puede entenderse desde diferentes enfoques. Uno de ellos es el enfoque político, el cual supone la "idea de que todos los habitantes del planeta, con independencia del país en el que hayan nacido y del lugar del globo en el que se encuentren deberían tener la menos el mismo núcleo básico de derechos fundamentales, los cuales además tendrían que ser respetados por todos los gobiernos. Desde luego, la forma en que ese núcleo básico podría plasmarse en los distintos ordenamientos jurídicos no tiene que ser uniforme para ser acorde con los principios de justicia; la historia, cultura y pensamiento de cada pueblo o comunidad puede agregar, y de hecho históricamente ha agregado, una multiplicidad de matices y diferencias al conjunto de derechos fundamentales que establece su respectiva Constitución". Carbonell, Miguel. 2004. *Los derechos fundamentales en México*. México, Comisión Federal de los Derechos Humanos, e Instituto de Investigaciones Jurídicas, UNAM.

mecanismos de control incluso en el sector privado (Ferrajoli, 2006).

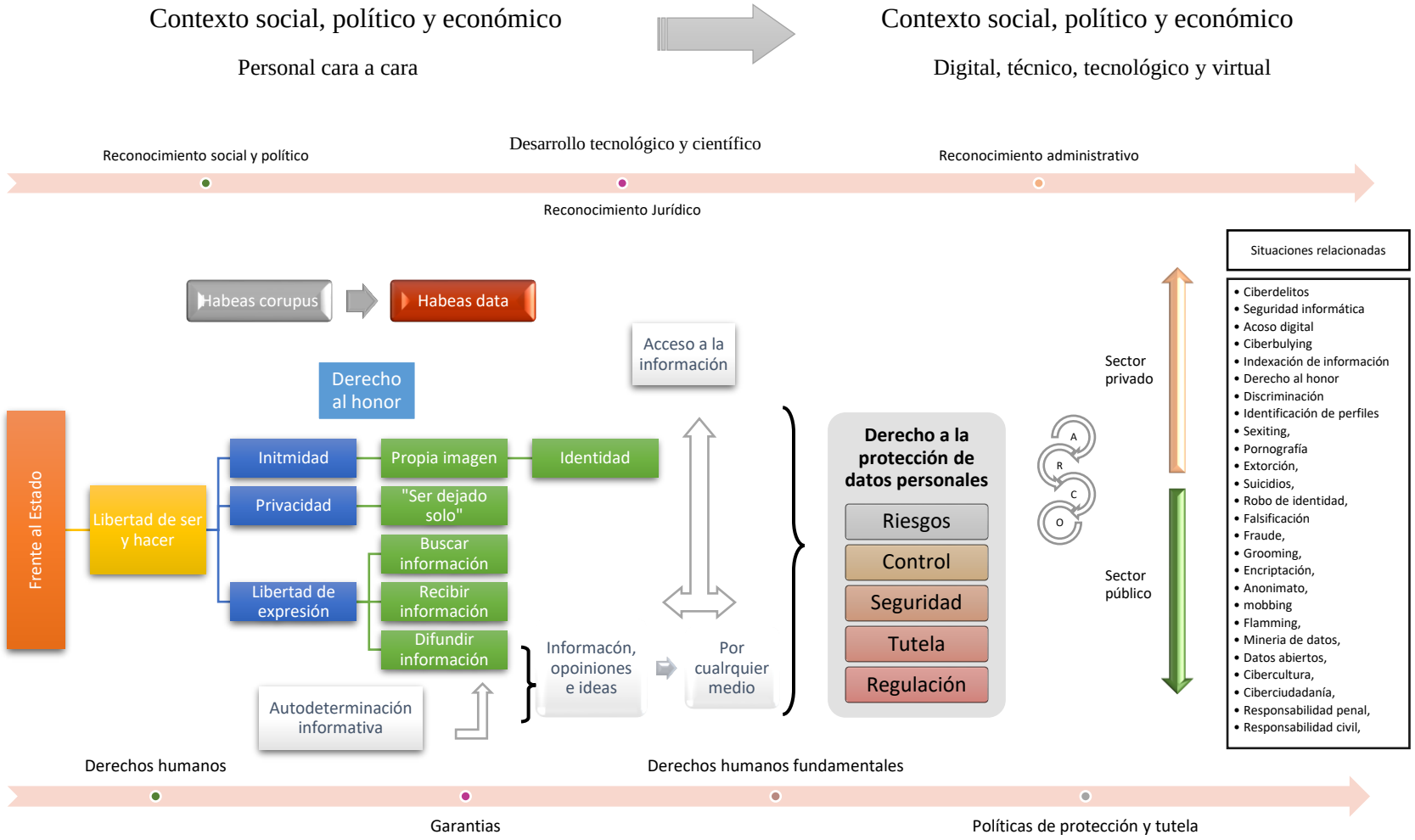
Dice Luigi Ferrajoli (2006) que "los derechos deben ser garantizados según su importancia". Hoy la protección de los datos personales es necesaria y relevante. La tecnología avanza, continúa potencializándose y todavía no alcanza su máximo esplendor. Ante este desarrollo, el derecho y las técnicas administrativas de protección están quedando rezagadas. Este es el contexto en el que surge el nuevo derecho humano, el cual se enfrenta a los intereses económicos nacionales e internacionales y a los avances tecnológicos.

Tres son sus principales fines: 1) asignar a la persona los derechos propiedad de sus datos; 2) definir la tutela de éstos, y 3) controlar su uso y tratamiento. Para lograr acciones concretas antes estas necesidades, primero se reconoce el derecho fundamental a la protección de datos personales (se plasma en tratados internacionales y en constituciones nacionales) y luego se crean garantías para proteger este derecho mediante un conjunto de normas secundarias. Es decir, se crean leyes generales, reglamentos, códigos y lineamientos para controlar los riesgos que implica el manejo de datos, los cuales a su vez se convierten en principios, procesos, procedimientos y estrategias de acción que definen el comportamiento y las formas de actuación de todos los involucrados en el tratamiento de los datos: el gobierno, las empresas y la persona, esta última por el sujeto de regulación y acción del Estado y el mercado.

Para lograr la regulación en la materia, se diseñaron y definieron las instituciones y las organizaciones encargadas de proteger el tratamiento de los datos personales, lo cual tuvo como objetivo modificar las conductas y las interacciones entre los actores implicados. En el esquema 2 de la siguiente página, se muestran las relaciones entre la protección de datos personales y otros derechos como el honor, el derecho a la propia imagen, la protección de la intimidad, de la privacidad, la autodeterminación informativa, el acceso a la información, el habeas corpus y el habeas data.[7] Este esquema también establece las interacciones entre la protección de datos personales y los ámbitos de protección y tutela, así como una lista no exhaustiva de temáticas vinculadas. Esto en aras de sistematizar los vínculos teórico-conceptuales en torno a la protección de datos personales.

[7] Para profundizar en el tema consultar: Cienfuegos Salgado, David. 2011. *El habeas corpus en México. Cuatro regulaciones en el ámbito local: Aguascalientes, Colima, Guerrero y Puebla.* Ponencia presentada en el Congreso REDIPAL, México, Cámara de Diputados. Y Bazán, Víctor. 2012. *El habeas data, su autonomía respecto del amparo y la tutela del derecho fundamental de autodeterminación informativa*. Anuario de derecho constitucional latinoamericano. Año XVIII. Pp. 37-76. Bogotá, Colombia

Esquema 2. La relación entre los derechos vinculados a la protección de datos personales.



Fuente: Elaboración propia

1.3 Niveles de protección

Si consideramos que cada esfera de la vida de las personas: pública, privada e íntima, contiene información diversificada en niveles de importancia, se puede definir que éstas requieren niveles de protección diferenciada. En este sentido, el tipo de protección está asociado al tipo de datos al que hace referencia. Hay tres tipos de protección: protección básica, de nivel medio y nivel alto. Éstas se relacionan con los tipos de datos de la siguiente manera:

a) *Protección básica.* Cuidado que se da a la información clasificada como pública, la cual debe estar disponible y archivada según los procedimientos de accesibilidad, comprensión y suficiencia. Esta información identifica a una persona, pero su transparencia es necesaria para lograr un bien colectivo, ejemplo las cédulas profesionales. Esta información nunca permite crear un perfil ampliado de la persona.

b) *Protección intermedia:* Resguardo de información privada que es utilizada para dar u ofrecer un bien o servicio que solicite o mediante el cual se beneficie a una persona. Esta información permite identificar a una persona porque así lo consintió de manera tácita o explicita, al disfrutar, solicitar o ejercer un bien, servicio o derecho.

c) *Protección alta*: Cuidado de la información altamente sensible. Este nivel engloba todos los datos personales más protegidos, como pueden ser las inclinaciones sexuales, origen racial, ideología, religión del sujeto, los datos genéticos y biométricos. Es información considerada como íntima y su tratamiento podría derivar en afectaciones graves para la persona en su ser, esencia y vida. La información que tiene esta categoría de protección revela las características más singulares de la persona y permite crear perfiles ampliados de la persona, por lo que no podrá ser tratada si no hay consentimiento explícito por escrito. De otra manera se estarían tratando de forma ilegal.

Esta clasificación de niveles de protección atiende a un criterio de clasificación de los datos personales de acuerdo al nivel de protección que requieren. Sin embargo, si partimos de esta idea estamos aceptando que los datos personales requieren niveles de protección diversificados. Es decir, que dependiendo del tipo de dato personal será el tipo de seguridad, cuidado y control. Esto tiene que tratarse con cuidado, para no caer en la simplicidad de que los datos clasificados como públicos no necesiten protección adecuada. El razonamiento más bien es que todo tipo de

información requiere parámetros de protección, cuidado y seguridad con estándares internacionales, sin embargo, las personas deben ser sumamente cuidadosas con la protección que le den a la información según su tipo.

Fausto Kubli (2008: 20-22), argumenta que "para el caso mexicano los datos que requerirán amplia protección y control serán los genéticos y los proteómicos. Esta información está clasificada como un dato altamente sensible. Esta sensibilidad implica reconocer que el uso inapropiado del conocimiento del material genético de la especie (persona) puede resultar indigno, en el sentido de dar lugar a discriminaciones o pérdida de la diversidad". Por eso es necesario crear controles desde el diseño institucional y organizacional con el objetivo de proteger de daño a las personas y a las futuras generaciones, más allá de una norma jurídica.

En parte, es importante reconocer que existen ámbitos diversificados de la información, donde dependiendo de la situación, el caso o el hecho se podrán clasificar como datos de uso común, sensibles y altamente sensibles. Los datos de uso común serían aquellos que se pueden encontrar en fuentes de acceso público. Los sensibles los podemos definir como toda aquella información privada que identifica o hace identificable a una persona bajo su consentimiento tácito o explicito, y los datos altamente sensibles corresponderán a los niveles más íntimos de la persona donde la identidad, el honor, la imagen humana y la psique individual toman forma. Es importante aclarar que esta clasificación es general y nunca absoluta, pues cada situación particular puede modificar el nivel de importancia, seguridad o sensibilidad de la información.

Una vez definido el derecho a la protección de datos personales y su contenido, es necesario conocer cuál es el fondo teórico por medio del cual se argumenta la intromisión del Estado como organismo regulador, capaz de garantizar el ejercicio, la tutela y protección de este derecho, mediante la creación de normas y estructuras de autoridad.

1.4 Estado y derechos

En este apartado se explican las acciones públicas que se han realizado en torno a la protección de los datos personales. Los vínculos conceptuales de este apartado son importantes porque se define el papel del Estado en torno a la regulación de los datos personales, el diseño institucional y organizacional, la innovación y la competitividad económica. Se parte de que el Estado para proteger los derechos humanos fundamentales crea las garantías jurídicas y organizativas necesarias por medio de las principales acciones que tiene para intervenir en las conductas

sociales: las acciones burocráticas, legales, discursivas y de filtraje internacional (O´Donnell, 2008: 89-99), buscando equilibrar intereses privados, colectivos y derechos humanos.

1.4.1 El Estado como garante de la seguridad y los derechos individuales

De acuerdo con Guillermo O´Donnell (2008: 91) el Estado liberal clásico justifica su existencia mediante cuatro principales dimensiones: a) eficacia de la burocracia, b) efectividad del sistema legal, c) credibilidad del discurso y d) el filtraje internacional. Estas dimensiones permiten, en menor o mayor medida, asegurar que el Estado cumpla con las funciones primordiales en un contexto moderno y con tendencia al ideal liberal. La primera, eficacia de la burocracia, parte del supuesto fundamental de que el "Estado es un conjunto de burocracias, que realizan acciones orientadas a cumplir algún aspecto del bien público, cuya custodia o promoción les ha sido institucionalmente encomendada. Se espera que las burocracias efectivamente cumplan con la misión que les ha sido legalmente asignada"

La segunda, efectividad del sistema legal, hace referencia al Estado como un sistema jurídico, el cual penetra, moldea y organiza innumerables relaciones sociales. Más que una "relación suma cero, es de suma múltiple y de mutua potenciación" (O´Donnell, 2008: 91), pues la legalidad efectiva, al organizar y moldear las relaciones sociales, potencia la sociedad y la ayuda a desplegarse, proveyéndola de bienes públicos, orden y previsibilidad de esas relaciones sociales.

La tercera dimensión es el discurso propio de la autoridad del Estado, que dicta ciertos valores y principios moldeando el comportamiento de su población. Es decir, se le atribuyen valores de forma legítima a la sociedad y este discurso provee al Estado de legitimidad. Esta es la dimensión de credibilidad del Estado. Una cuarta dimensión, muy vinculada a esta última, es que el Estado pretende ser un filtro eficaz. Es decir, el Estado funge como intermediario entre la población que delimita territorialmente y lo externo, argumentando que abre o cierra sus fronteras físicas o invisibles por el beneficio público. Así invita, permite o rechaza influencias del contexto internacional al nacional (O´Donnell, 2008: 91). En este sentido, el Estado a partir de un apartado administrativo, jurídico e ideológico hace cumplir los acuerdos sociales que permitan el desarrollo social y económico tanto del interés colectivo como del individual.

En el marco de un Estado democrático y de derecho[8] podemos entender su intervención en la

[8] *Rule of law*, *Rechtsstaat* y *État de Droit*: El origen de este concepto es el de *Rechtstaat* prusiano, que no tenía nada de democrático. Este *Rechtsstaat* fue un intento exitoso de legalizar y regularizar las relaciones del gobierno básicamente con los Junkers y con la burguesía alemana, así como de regularizar las relaciones al interior de la

garantía de los derechos políticos auspiciados por la democracia (O´Donnell, 2008: 93), mediante límites efectivos al ejercicio de la autoridad para salvaguardar los derechos y libertades del ciudadano (Tortora, 2010). Sin embargo, esa imposición de límites suele ser débil como en el caso de América Latina (incluyendo México) porque coexisten democracias políticas con una legalidad estatal que no cubre todo el territorio ni toda la población. O´Donnell (2008: 95) denomina a estos espacios las *zonas marrones*, donde la legalidad del Estado es remplazada por las diversas legalidades mafiosas (informales), que son las que realmente gobiernan las relaciones sociales en extensos territorios. Tenemos entonces un Estado deficiente en la dimensión de la legalidad, las sanciones y la rendición de cuentas. De allí la necesidad de expandir las exigencias para la democracia y su calidad, pues estas deficiencias afectan gravemente el ejercicio, las acciones del gobierno y su legitimidad.

Otro aspecto importante de resaltar es que "existe también un serio riesgo de mitificación del Estado de Derecho y el concepto de legalidad. Es decir, bajo la democracia, la legalidad del Estado promueve la igualdad y respalda la defensa de los derechos, pero por otro lado dicha legalidad, al mismo tiempo, con el mismo lenguaje y frecuentemente con las mismas autoridades, sanciona y respalda eficazmente la continua reproducción de importantes desigualdades" (O´Donnell, 2008: 95; Kelsen, 1960 y Hart, 1961). Es digamos, la reproducción de un doble papel. Por un lado, la defensa de los derechos y por otro la reproducción de las desigualdades a través de las legalidades de la ley. Este aspecto de la legalidad es sumamente importante, porque como lo dicen los autores citados, se pueden presentar casos donde la legalidad respalde, más que acciones de protección a la persona, desigualdades y afectaciones graves.

De manera que cuando hablamos de régimen democrático ya estamos hablando de un Estado que incluye tanto dimensiones legales como garantías a los derechos ciudadanos, pero también estas normas formales se vuelven límites a la conducta de terceros (O´Donnell, 2008: 95). Hasta aquí hemos explicado que, si bien el Estado actúa por medio de sus principales cuatro funciones, cuando se habla del Estado democrático de derecho se amplían éstas con la capacidad de sanción para garantizar los derechos, exigir rendición de cuentas y mantener la legalidad de la ley. Entonces, a partir de estas siete dimensiones podemos derivar las acciones gubernamentales que buscan proteger a los individuos y garantizar sus derechos por diferentes vías: la implementación

creciente compleja burocracia prusiana y reafirmar la legalidad de diversas relaciones civiles y comerciales. Para profundizar ver: Grote, Rainer. 2002. *Rule of Law, Rechtsstaat, y Etat de Droit. En Pensamiento Constitucional, Año VIII Número 8, Disponible en http://www.revistas.pucp.edu.pe/index.php/pensamientoconstitucional/article/viewFile/3277/3118*

de normas, límites y sanciones; incluso mediante procesos administrativos específicos. Donde Estado y gobierno interactúan en busca de proteger tanto los derechos colectivos como los individuales.

1.5 El gobierno, la información y los datos personales

David Arellano y Felipe Blanco (2016: 19) dicen que el gobierno es "el encargado de establecer y regular el marco social en el que los ciudadanos nos desenvolvemos todos los días". El gobierno como uno de los pilares del Estado está definido por un aparato administrativo que se encarga de ejecutar las decisiones, las acciones y de asumir las consecuencias que dan marco a la vida institucional y organizacional de toda política pública.

> "El gobierno, es el depositario de las funciones del poder del Estado, es decir, de las funciones públicas cuyo ejercicio se distribuye entre las diferentes instancias del aparato gubernamental del Estado. En la tesis organicista, el gobierno viene a ser el cerebro del Estado, dado que conduce, rige y dirige su actuación. En una aproximación al concepto de gobierno, diré que, en sentido amplio, el gobierno es el conjunto de órganos depositarios del poder público, cuyos titulares ejercen, en consecuencia, las funciones públicas respectivas; y en sentido restringido, el gobierno es el órgano o conjunto de órganos depositarios del Poder Ejecutivo." (Fernández, 2015: 50).

Por gobierno no sólo se entiende a la administración pública como el aparato administrativo del Estado (Guerrero, 1986), sino también a otros órganos del Estado con funciones políticas y toma de decisiones pública, como los poderes legislativos, judiciales, y de relaciones institucionales entre el Estado y la sociedad, como los organismos hoy denominados autónomos. El gobierno utiliza diferentes herramientas y recursos para cumplir con sus funciones y para tomar decisiones. Principalmente se rige por todo el sistema jurídico que lo faculta para hacer o no hacer; pero también, por ser una estructura de autoridad estatal, se guía por un conjunto de normas informales que le permiten actuar, incluso más allá de las normas establecidas; en teoría siempre en busca de soluciones a los problemas representativos para los diferentes agentes sociopolíticos.

Un elemento que el gobierno siempre ha tenido como un insumo para la toma de decisiones ha sido la información. Karl Deutsch (1971) concibe al gobierno como un proceso de decisiones fundado sobre flujos variados de información. De acuerdo con esta concepción, los mensajes provenientes del entorno interno y externo tienen numerosos y variados receptores. Esta noción

de receptores abarca diversas funciones como son la codificación, la selección de información y el procesamiento de datos (*data processing*). En este sentido cualquier gran sistema político o administrativo debe alimentarse con insumos de información que se transmiten a través de diferentes canales de comunicación.

Desde la antigüedad la información ha sido indispensable para que los gobiernos tomen decisiones. El censo fue uno de los primeros mecanismos para la recolección y sistematización de la información, así como las listas de contribuyentes. Sin embargo, como bien lo identifica Karl Deutsch, a partir de los años 70 y en los años posteriores el uso de la información se potencializó debido a la ampliación de los canales de comunicación. La computadora, los sistemas informáticos y en general el desarrollo de las tecnologías de la información y la comunicación (TIC) dieron como resultado el tratamiento automatizado de información. Contexto ante el cual el gobierno se ha visto en la necesidad de incorporar estas nuevas herramientas en la toma de decisiones para la provisión de bienes y servicios públicos con mayor alcance y en menor tiempo.

En principio el gobierno posee datos e información sobre las personas que habitan en el territorio del Estado o que pertenecen a éste. Es decir, sobre las personas que se encuentran formalmente dentro, fuera y en tránsito del territorio. "Datos que van desde aquellos que identifican a una persona, hasta los más íntimos, como sus orígenes familiares, su salud y posibles minusvalías; su itinerario educativo, sus antecedentes penales, sus ingresos, sus propiedades, etc. Toda esta información obra en poder del gobierno" (Guichot, 2007: 408).

Con el desarrollo de las TICs la administración gubernamental se vio en la necesidad de reconocer nuevas maneras de gobernar e interactuar con los ciudadanos, reconociendo lo que Helen Margetts (2008) llama la segunda ola "del gobierno en la era digital", la cual consiste en la integración de las funciones gubernamentales con la tecnología y los nuevos retos de seguridad a los cuales se va a enfrentar, bajo lo que Jane E. Fountain (2013: 108) denomina:

> "El cambio institucional hacia el Estado virtual con el uso de tecnologías de la información. Donde el Estado se enlaza cada vez más por medio de sistemas de información, acuerdos interdepartamentales e intergubernamentales, asociaciones público-privadas, interacción con administraciones públicas federales, estatales, locales; organizaciones privadas con y sin fines de lucro, las cuales comparten servicios basados en la web que ofrecen los espacios virtuales del gobierno y de cientos de organizaciones privadas. Estas interacciones virtuales se presentan en partes diversas, jurisdiccionalmente separadas y muchas veces geográficamente lejanas."

En este contexto digital, la información que se requiere para ofrecer tanto servicios públicos como privados ya no sólo se encuentra en espacios físicos definidos que compliquen su tratamiento. Esta información ahora es digital y con el uso de las herramientas computacionales su tratamiento se facilita, incrementando la necesidad de información para brindar más y mejores servicios.

El gobierno, entonces, utiliza la información para la toma de decisiones, pero esta información ya no sólo es aquella que permite conocer las características esenciales de su territorio; de su estructura gubernamental, de sus procesos y procedimientos administrativos, sino también información de las personas a las que gobiernan y más aún, de información que muchas veces no está en posesión del sector público sino de particulares, como es el caso de las empresas.

1.5.1 El control gubernamental de la información personal

El gobierno como expresión institucional de la autoridad del Estado tiene como parte de sus funciones elaborar, ejecutar y sancionar las normas del comportamiento social a través de órganos administrativos legalmente constituidos. Dentro de las herramientas para tomar decisiones públicas se encuentran las legislativas, las judiciales y las ejecutivas. A través de la administración pública toma diversas decisiones: asigna recursos, socializa valores; crea agencias de Estado y otras agencias de gobierno; controla, fiscaliza, vigila, da seguridad; distribuye derechos y obligaciones; elimina controles; exige impuestos, regula acciones económicas, políticas y sociales de terceros, etc. Estas acciones son políticas públicas ejecutadas por órganos de la administración pública. Algunas directamente emanadas de la acción del gobierno (políticas gubernamentales), otras con respaldo público y de sectores sociales (políticas sociales) y otras que surgen como necesidades sustantivas del Estado a partir de intereses nacionales (políticas de Estado). Cada política tiene ciertos principios, objetivos y fines (Majone, 1989), así como restricciones y consecuencias. Las políticas públicas tienen la ventaja de ser una acción que implica la participación de diversos actores involucrados, atiende problemas específicos e invariablemente cuenta con la participación del Estado (Merino y Cejudo, 2010). En resumen:

> “Las políticas públicas aluden a situaciones que combinan: la oferta y los resultados de gobierno; la acción y no acción de éste valorando condiciones, actores, tiempos, demandas y presiones públicas; las decisiones y las acciones que se rehacen de manera continua tomando en cuenta el juego de intereses, la opinión pública, los valores que competencia, las demandas y la sinergia de los acores sociales y políticos; la

> intencionalidad para planificar e implementar estrategias; la combinación de ámbitos, responsables, órdenes, legislación, oficinas, participación, corresponsabilidad, recursos, personal directivo y operativo; y las visiones de corto, mediano y largo plazos para cumplir objetivos y metas que tendrán impacto diferenciado en el espacio público" (Uvalle, 2011: 3).

Entonces, las políticas públicas son acciones del gobierno que se ejecutan a través de la administración pública. Estas políticas tratan de solucionar problemas colectivos, "desactivar tensiones, regular problemas y definir soluciones que eviten la alteración violenta de la correlación de fuerzas" (Uvalle, 2011: 3). Asimismo, una política pública también garantiza y protege derechos, por lo que una política pública puede tener uno o varios fines y vincularse con otros problemas o situaciones que originen consecuencias inesperadas, tanto positivas como negativas.

En México las políticas nacionales dirigen y generalizan principios a toda la comunidad política que integra el Estado. En la Constitución Política de los Estados Unidos Mexicanos (CPEUM, 2017) se reconoce la rectoría del Estado en el desarrollo nacional (Artículo 25), en la planeación nacional (Artículo 26), y en la provisión de servicios y derechos (artículos 1 al 29). En este sentido, el gobierno tuvo que actuar en torno al uso y tratamiento de los datos personales tanto en el sector público como en el privado. De allí que se haya diseñado una política para la protección de estos datos.

1.6 La protección de datos personales como política pública

Estudiar las acciones del gobierno mediante las políticas es poner "énfasis en los problemas fundamentales del hombre en sociedad" (Laswell, 1951: 89); "en los actos y no actos de una autoridad pública frente a un problema o servicio relevante de su competencia; en las actividades de una autoridad pública investida de poder y de legitimidad gubernamental; en los programas de acción gubernamental en un sector de la sociedad o en un espacio geográfico" (Meny y Thoenig, 1992: 89); en la argumentación y persuasión de las políticas (Majone, 2005 [1989]); en los valores, fines y prácticas que proyecta un programa (De León, (1997). Esto, y más, pretende realizar el estudio y análisis de las políticas con el objetivo de resolver "problemas públicos que platean al gobernante las opciones disponibles y evalúan sus consecuencias por medio de modelos matemáticos u otras técnicas de análisis" (Majone, 2005 [1989]: 57).

Es decir, una política pública: a) es un conjunto de acciones estructuradas en modo

intencional y causal, que se orienta a realizar objetivos considerados de valor para la sociedad o a resolver problemas cuya solución es considerada de interés público; b) acciones cuya causalidad e intencionalidad han sido definidas por la interlocución entre el gobierno y los sectores de la ciudadanía; c) acciones decididas por autoridades públicas legítimas; d) acciones ejecutadas por actores gubernamentales en asociación con actores sociales, y e) acciones gubernamentales que dan origen o forman un patrón de comportamiento del gobierno y la sociedad.

> "Lo distintivo es el hecho de integrar un conjunto de acciones estructuradas, estables, sistemáticas, que representan el modo en el que el gobierno realiza de manera permanente y estable las funciones públicas y atiende los problemas públicos: un patrón de actuación. Dicho de otra manera, lo específico y peculiar de las políticas públicas consiste en ser un conjunto de acciones (o inacciones) intencionales y causales, orientadas a la realización de un objetivo de interés y beneficio público, cuyos lineamientos de acción, agentes, instrumentos, procedimientos y recursos se reproducen de manera constante y coherente. La estructura estable de sus acciones durante un cierto tiempo es lo específico y lo distintivo de ese conjunto de acciones de gobierno es lo que llamamos políticas públicas" (Aguilar, 2010: 29).
>
> "Alrededor de una política pública se enlazan leyes, poderes públicos, actores políticos y sociales, recursos financieros y procesos administrativos" (Aguilar, 2010: 30). "La política pública bien entendida exige un proceso racional, informado y comprometido de selección y definición del problema que trata de resolver, a partir de los medios efectivamente disponibles para solucionarlos. Y supone también, que desde el momento de adoptar una determinada definición, han de plantearse también los resultados que se desean obtener y el proceso a través del cual serán conseguidos" (Merino, 2013: 36).

En este sentido:

> "Las políticas públicas consisten en la utilización de los medios que tiene a su alcance el Estado para decidir en qué asuntos intervendrá y hasta qué punto y con qué medios lo hará. Son decisiones del Estado que se originan en un proceso político previo mediante el cual se seleccionan y se definen problemas públicos; decisiones políticas, pues a pesar de todas las debilidades que haya mostrado el Estado durante los últimos años, sigue teniendo el monopolio legítimo de la coerción física, sigue siendo el eje de la organización

política de la sociedad y sigue produciendo las normas a través de las cuales se organiza la convivencia.

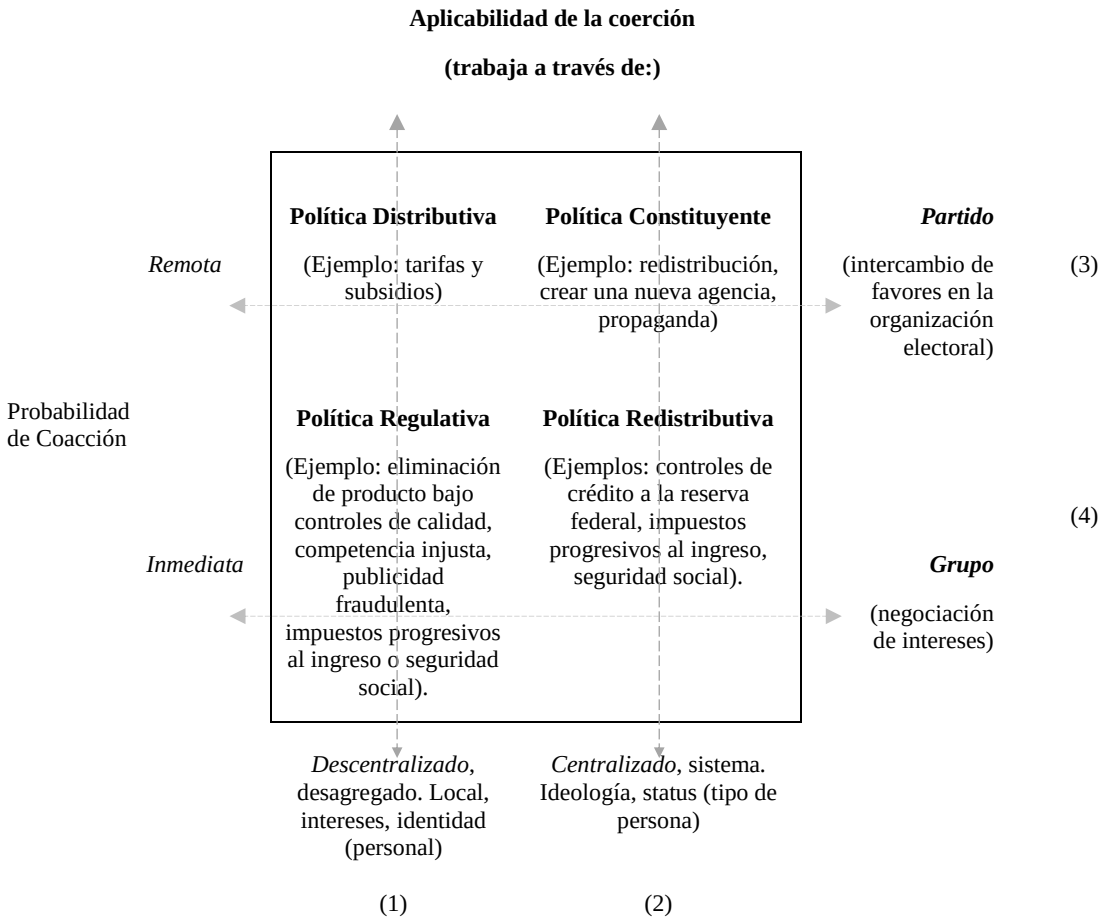
> "De modo que tras las políticas públicas hay decisiones de poder, tomadas por el Estado o bajo el cobijo de las normas y de las estructuras de autoridad generadas por esa organización política. Decisiones que reclaman del Estado la selección de problemas públicos y de distintas alternativas de acción para modificar el *statu quo* que le motivó actuar" (Merino, 2013: 37).

Con esto comprendemos cómo la participación del Estado es fundamental en la elección y diseño de las políticas públicas. Éstas pueden ser decisiones basadas en intereses diversos y dirigidos a solucionar una o varias situaciones más o menos incluyentes. Algunas serán acotadas, específicas y dirigidas a solucionar problemas más o menos simples, otras más elaboradas para tratar problemas complejos. La política pública no es una, ni de un tipo. Existen diversas políticas públicas; políticas que pretenden por sus mismos fines y objetivos ser diferentes.

Theodore J. Lowi (1964, 1972, 1998: 2) identifica cuatro tipos de políticas que modifican el comportamiento de los agentes sociales, económicos y políticos. Él deriva cuatro tipos de actuación del Estado como autoridad: actuación con políticas distributivas, redistributivas, constitutivas y regulativas. Cada una promueve uno o varios tipos de interacciones entre actores, procesos, decisiones y soluciones. Esta tipología es planteada por el autor mediante la combinación de dos criterios: la estructura de coerción utilizada por el poder público y el efecto que sobre los individuos tiene la intervención realizada.

En el esquema 3 se pueden observar las diferentes relaciones que implican decisiones e imposiciones que varían entre sí, de acuerdo a la clasificación de Lowi.

Esquema 3. Tipos de políticas y estructura de coerción.



Fuente: Lowi, 1972: 300. (Traducción propia)

Cada tipo de política establece ciertas modificaciones o patrones de conductas; tiene objetivos específicos, y efectos en las obligaciones, los privilegios y los poderes que otorga.

a) "**Las políticas distributivas** establecen privilegios con base en conductas individualizadas; es decir, confieren facilidades o privilegios, como por ejemplo un subsidio al uso de un bien como el agua, el salario mínimo o la canasta básica. Este tipo de políticas imponen clasificaciones o estatus, como por ejemplo la política fiscal (impuesto de la renta progresivo) y la seguridad social.

b) **Las políticas constitutivas** son las que establecen las reglas de la distribución de poderes en un entorno social, generando los procedimientos para la adopción de las decisiones públicas; por ejemplo, la creación de una agencia gubernamental.

c) **Las políticas redistributivas** transfieren recursos de unos grupos de individuos, regiones o países a otros, es decir, otorgan beneficios a unos grupos sociales repercutiendo los costes correspondientes sobres otros grupos; incluyen también la provisión de determinados bienes que el gobierno insta a consumir como la educación elemental o la salud pública.

d) **Las políticas regulativas** tienen por objetivo motivar cambios inmediatos, dirigidos a la conducta individual, donde se es más susceptible de incorporar intereses o negociaciones de grupo y las acciones tienden a ser descentralizadas, dirigidas por intereses particulares o individuales" (Lowi, 1972: 300).

Estas últimas políticas imponen obligaciones para modificar una o varias conductas específicas; por ejemplo, la intervención en la economía o la legislación en materia de salud. Estas políticas son formuladas por una autoridad gubernamental con la intención de influir en la conducta de los ciudadanos, individual o colectivamente, mediante el uso de acciones punitivas, imponiendo obligaciones y generando sanciones en caso de transgresión. Estas acciones se suponen con un impacto "casi inmediato" en la conducta individual o en la conducta que regulan (Lowi, 1972).

Las acciones tendientes al control y uso de los datos personales pertenecen a una política regulativa, porque es una acción derivada de decisiones políticas, negociaciones de grupos, de intereses y tendientes a descentralizar y desagregar esos intereses, así como a someter a la conducta individual o de grupo (empresas o gobierno) de manera más o menos inmediata. Esta política tiene sus instrumentos instruccionales y organizacionales específicos, como los valores, normas y conductas que rigen el tratamiento de los datos personales (marco institucional) y las agencias de control, autoridades de control u órganos de gobierno jurídicamente constituidos, que ejecutan y toman decisiones en torno al tratamiento de los datos (marco organizacional).

1.6.1 Instrumentos institucionales

Las instituciones entendidas como las reglas del juego son un instrumento que permite a los gobiernos dirigir las conductas sociales: individuales y colectivas. Son las limitaciones ideadas por el hombre que dan forma a la interacción humana y estructuran incentivos en el intercambio, sea político, social o económico. Las instituciones incluyen cualquier forma de restricciones que los seres humanos idean para las diversas formas de interacción humana: formales e informales (North, 1990).

Entonces, éstas "definen y limitan el conjunto de elecciones de los individuos, y su violación o falta de aplicación implican un castigo" (North, 1990: 3-4). "Las instituciones proporcionan el marco general para el intercambio y dependen de la motivación de los participantes, la complejidad del medio y la habilidad de los participantes para interpretar y ordenarlo; para su mediación y cumplimiento obligatorio" (North, 1990: 51). De esta manera se entiende que el conjunto de reglas formales e informales, su tipo y la eficacia de la aplicación moldean todo el carácter del juego; el comportamiento individual y colectivo. El éxito de la aplicación de las normas estará dado por la reputación de los jugadores, la eficacia de la vigilancia y la gravedad de las sanciones.

Todas las reglas se comportan en un marco superior: el marco institucional, que está integrado por normas supremas y códigos de comportamiento general. Todas las instituciones varían en cuanto a complejidad, desde aquellas que facilitan el intercambio simple hasta aquellas otras que se extienden a numerosos individuos y a lo largo del espacio y del tiempo. De esta manera, el marco institucional respectivo está dado por el conjunto de normas legales, organizacionales, cumplimiento obligatorio y normas de conducta (North, 1990: 51).

Las instituciones en la sociedad reducen la incertidumbre porque establecen una estructura estable en las relaciones humanas. Esta estabilidad no implica que no se modifiquen, al contrario: las convenciones, los códigos de conducta, las normas de comportamiento de la ley estatutaria, las leyes consuetudinarias, las costumbres y los contratos entre particulares siempre están evolucionando y, por lo tanto, están alterando continuamente las opciones disponibles entre los diferentes tipos de interacciones. Los cambios pueden ser lentos y graduales en el comportamiento, y en muchas ocasiones sólo el devenir histórico puede percibirlos.

La institución como mecanismo de control suele estar plasmada en la Constitución, moldeada en leyes, reglamentos y lineamientos de procesos y procedimientos. A este mecanismo se le denomina regulación institucional, a partir del diseño constitucional. Sin embargo, también existen otras dos herramientas institucionales que están vinculadas a un contexto global de libre mercado y tendiente al respeto de la competitividad económica: la desregulación y la autorregulación (Jordana y Levi-Faur, 2004). Estos mecanismos son las reglas de juego que limitan o permiten ciertas conductas.

La desregulación no quiere decir que nos encontremos ante la ausencia absoluta de regulación, sino que se trata de un tipo distinto de regulación a la ya descrita. El supuesto inicial es buscar que el mercado actúe libremente en el juego natural de la oferta y la demanda (Joskow,

2004); con retraimiento del Estado en toda la actividad económica privada, limitando su actuación a aquellos casos en los que se producen las llamadas fallas de mercado, o cuando se dan situaciones de ausencia de mercado.

Como observó Majone (1997), los gobiernos modernos occidentales han experimentado un cambio fundamental, pasando de un Estado positivo (en donde los gobiernos intervinieron directamente con el fin de lograr un conjunto de beneficios sociales y metas económicas), a un Estado regulador (donde la prestación de servicios es directamente subcontratada por terceros, a los cuales el gobierno trata de controlar e influir a través de una mezcla de arreglos contractuales, normas y regulaciones). Con esto podemos diferenciar entre la regulación y la desregulación. En la primera las normas son restrictivas y en la otra son permisivas. Esta idea de desregulación viene acompañada con la denominada gobernanza regulatoria o capitalismo regulador (Comisión Federal de Mejora Regulatoria (COFEMER, 2010) en donde es necesario aumentar la confianza en el mercado como el vehículo para la riqueza individual, la maximización y la prestación de los servicios públicos.

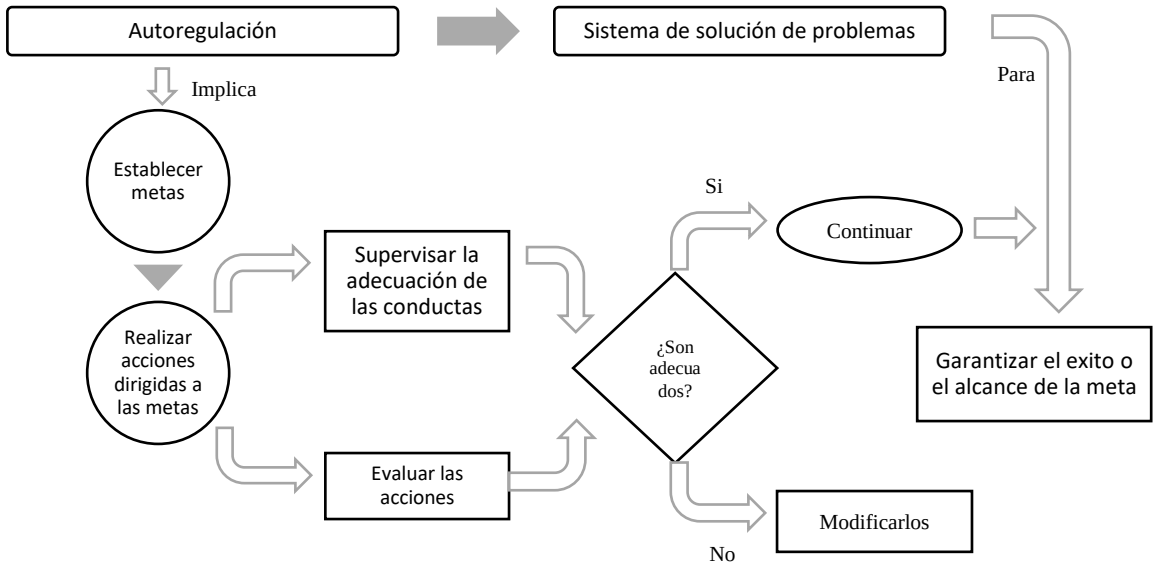
La diferencia entre regulación y desregulación nos muestra los cambios acontecidos en la función reguladora del Estado. Al final obedece a un contexto específico. En resumen, radica en que la desregulación obedece a los procesos de privatización promovidos desde la década de los años 70 (Joskow, 2004), donde las empresas públicas disminuyeron considerablemente y se transmitieron servicios al sector privado y la regulación obedece a la necesidad del gobierno por intervenir en el nuevo juego (y sus reglas) que se originó con dicha privatización. Entonces esta nueva regulación permite regular la conducta de los nuevos actores del juego, buscando la eficiencia y la mejora en la productividad (COFEMER, 2010). Otra de las herramientas de la política regulativa es la autorregulación.

La etimología latina de autorregulación nos dice que es “el proceso de regular el actuar por sí mismo o sobre sí mismo” (RAE, 2019). De esta manera, la autorregulación es la capacidad que tiene un sujeto, o una institución, organización o asociación, de regularse a sí misma bajo controles voluntarios. Esta herramienta es fundamental para comprender el comportamiento económico y político porque nos ayuda a entender, por ejemplo, la forma como se organiza la protección de datos personales en los Estados Unidos de América, donde la mayoría de las empresas siguen el esquema de la autorregulación. Es decir, crean códigos de conducta vinculantes a partir de los cuales pretenden conseguir la confiabilidad de sus clientes.

Esta herramienta ha sido utilizada por los hacedores de políticas con el objetivo de promover

la acción y el control por parte de los propios agentes regulados. Pero además es una práctica que reconoce los límites de los actores; disminuye costos de tiempo y recursos al dejar cierta discrecionalidad en los parámetros de control. En este sentido, las actividades autorreguladoras son procesos internos en las organizaciones, con el objetivo de obtener beneficios positivos para su organización. El proceso puede verse de la siguiente manera:

Esquema 4. Proceso de autorregulación.



Fuente: Elaboración propia.

En este sentido el sistema de autorregulación es un conjunto de normas, compromisos éticos y principios de acción que vinculan el hacer de las organizaciones sin que medie una norma jurídica que imponga obligaciones. Aquí la organización crea controles propios que limitan su acción, con el objetivo de cumplir responsablemente sus metas y objetivos sin dañar a terceros, es decir, sin ocasionar daños al interés público y colectivo (Jordana y Levi-Faur, 2004). Este es el supuesto teórico que permite la generación de mejores prácticas en los actores para cumplir las normas a partir de parámetros, pero profundizando en las acciones necesarias para lograr resultados superiores que tengan beneficios positivos para la organización.

En México, los mecanismos de autorregulación han definido en dos tipos: autorregulación vinculante y no vinculante. Las primeras incluyen que pueden ser consideradas como una regla formal y reconocida tanto por el actor regulado como por el regulador y el segundo caso sólo son

acciones que el regulador recomienda considerar como acciones que pueden generar beneficios organizacionales. Como se ha visto, las políticas regulativas tienen diferentes herramientas mediante las cuales diseñan normas de comportamiento que les permiten modificar la conducta de los actores. Este es el diseño de instituciones.

1.6.1.1 El diseño de las instituciones

Un primer acercamiento del diseño institucional nos dice que es un proceso mediante el cual se idean, figuran, estructuran y crean instituciones para modelar comportamientos y conductas, que den solución a problemas públicos. Por lo tanto, se analizará el proceso de idear, modelar, estructurar y crear las instituciones formales que serán las reglas del juego (North, 1970) y que hacen referencia a las conductas individuales o colectivas, valores y principios definidos en constituciones, leyes, códigos o lineamientos normativos, mismos que tratarán de resolver la incertidumbre ante el tratamiento de datos personales en México.

Roberth E. Goodin (1996: 45) dice que "las instituciones no surgen de manera accidental, éstas a menudo son el resultado de actividades intencionales que pueden ser subproductos imprevistos, derivados de ciertas acciones intencionales mal dirigidas o simplemente de un error." En este sentido las instituciones son el resultado que surge indirectamente de la intencionalidad, es decir "una institución puede ser efecto de la acción intencional sin ser literalmente el producto deliberado de la acción de alguien". Hay, entonces una intención de por medio, pero las instituciones son el producto de otras circunstancias imprevistas, accidentales, contextuales. "No existe un único diseño ni un único diseñador. Se trata de una gran cantidad de intentos localizados de diseño parcial que se superponen entre sí" (Goodin, 1996: 46). Suelen diseñarse, más que instituciones, "planes para la construcción de instituciones, los cuales deberán tener adecuadamente en cuenta la multiplicidad de diseñadores y la naturaleza inevitablemente mezclada de sus intervenciones e intenciones en el proceso de diseño" (Dryzek, 1990: 40-50).

La intencionalidad en el diseño y en la construcción de las instituciones no suele ser el motivo y el resultado final de las mismas: "en los casos en los que el diseño directo resulta imposible, el diseño indirecto a menudo resulta practicable". El diseño indirecto reconoce la existencia de la intencionalidad, pero también de los errores y accidentes, motivo por el cual flexibiliza la intencionalidad originando un diseño controlado entre lo planeado y el devenir de la realidad. Entonces la intencionalidad se vuelve un mecanismo de control que permite en el diseño de

instituciones moldear los accidentes y dirigir la lógica propia de las instituciones: “los accidentes ocurren, pero la frecuencia y tendencia de estos accidentes pueden ser moldeadas en una medida significativa por las intervenciones intencionales de los responsables del planteamiento social” (Perrow, 1984).

En el área de políticas públicas el diseño equivale a la generación de opciones para la solución de problemas públicos: la opción de nuevas soluciones, a través de la combinación creativa de la recopilación y la innovación, y un compromiso serio tanto con los valores como con los contextos (Wildavsky, 1979; Brobrow y Dryzek, 1987). A menudo, el tema central en el diseño de políticas es la factibilidad, es decir, la posibilidad de implementación de diversas y posibles opciones a partir de la disponibilidad de recursos e incentivos con que cuentan diversos agentes y agencias que necesariamente deberán estar involucrados con la puesta en práctica de las intenciones de quienes determinan las políticas (Wildavsky, 1979, Linder y Peters, 1987 y Schneider e Ingram, 1993). En este sentido, se considera que los contextos, los intereses y las intenciones, la discusión, las opciones disponibles, así como los valores conjugados con el proceso de información e innovación, serán en parte los elementos que se habrán de considerar, en principio, en el proceso de diseño de las instituciones.

En la construcción de las instituciones las “intenciones de los agentes sociales para moldear las instituciones de determinada manera y no de otra” juegan un papel fundamental, pues “en la medida en que estén convencidos de tales argumentos y se sientan movidos por tales razones, esos agentes sociales intentarán poner en práctica sus prescripciones”. Ahora bien, otro “concepto fundamental del diseño, se refiere a la justa correspondencia del objeto diseñado con su entorno. Esto quiere decir que una institución bien diseñada sería aquella que resulte coherente en el entorno interno y externo, es decir, en armonía con el resto del orden social en el cual se inserta. Considerando el entorno colectivo e institucional, el moral individual y reconociendo la posibilidad de que existan buenas razones para procurar instituciones que se ajusten mal y no bien, al resto de su entorno” (Goodin, 1996: 56). Dentro de las razones internas están: las creencias, los deseos, los principios, los prejuicios y objetivos de la organización y como razones externas las verdades morales más generales, no vinculadas a creencias y deseos individuales.

Un buen diseño puede equipararse con la promoción de un funcionamiento sin tropiezos del objeto diseñado y del sistema más amplio en el que está inserto. Sin embargo, la falta de armonía no es del todo negativa, por eso es una buena técnica en el diseño designar a un agente que desafíe los propuestos compartidos entre los agentes diseñadores. La falta de armonía permite, en

ocasiones, retroceder un paso para poder avanzar dos, respecto al buen criterio, dice John Elster (1979). Entonces no se puede llegar a decir con certeza lo que es o no un buen diseño. El diseño institucional es un conjunto de acciones donde se definen normas y comportamientos; se prevén acciones, accidentes, situaciones inesperadas, pero difícilmente se puede tener el control absoluto de las instituciones y su entorno. Se trata, por lo tanto, de idear proceso y procedimientos que disminuyan la incertidumbre y definan de la manera más clara posible las relaciones entre actores en justa correspondencia con "los objetivos internos y el entorno inmediato" (Goodin, 1996: 58).

Por lo tanto, el diseño de una institución debe considerar que "los seres humanos son falibles y que las sociedades cambian". Resulta factible diseñar las instituciones de manera que atiendan los siguientes principios: sean *flexibles*, con el fin de admitir la posibilidad de "aprender con la experiencia y de evolucionar con el tiempo". Exista la posibilidad de *revisión* para permitirse atender nuevos parámetros. Exista *solidez*, con el cual las instituciones deben tener la capacidad de adaptarse a nuevas situaciones, y no resultar inelásticas o fáciles de desmoronar. Deben cambiar sólo en los casos en que se produzca cierto cambio fundamental en el universo fáctico o evolutivo, y deben sufrir únicamente adaptaciones superficiales a las nuevas circunstancias (Goodin, 1996: 61) para tratar de adaptarse a los cambios críticos del sistema, pero tener la solidez suficiente para proteger su esencia.

Otros principios que se deben considerar en el diseño institucional es la sensibilidad a la complejidad motivacional, la cual refiere cambios en los motivos que movilizan a la mayoría de los individuos. El principio de publicidad en el diseño institucional permite justificar a las acciones institucionales públicamente, es decir justificarlas con base en criterios superiores: "motivos superiores como razones de acción" (Mill, 1997 [1859]: 81) y evitar decisiones personalistas y egoístas. El principio de publicidad le da su fundamento colectivo; sin embargo, la cuestión de que esta premisa sea correcta o no para el diseño institucional depende de temas profundamente contenciosos que admiten solamente una resolución política, en última instancia (Goodin, 1996: 63).

Finalmente, contar con procesos de ensayo, error y aprendizaje permite perfeccionar los acuerdos institucionales, esta característica se fundamenta en el principio de *variabilidad*, donde se debe alentar la experimentación con diferentes estructuras en lugares distintos, además de alentar la reflexión acerca de las lecciones de otros y la disposición a aceptar tales lecciones cuando resulten adecuadas. El federalismo es defendido algunas veces precisamente sobre esta base, como laboratorio social en el cual se permite que emerjan enfoques diferentes en diferentes jurisdicciones

(Wildavsky, 1979).

Un sistema administrativo federal suele ser un espacio de experimentación institucional que permita el perfeccionamiento de las instituciones, aunque también puede ser una restricción para homogeneizar los acuerdos institucionales y el intercambio de experiencias. Otro peligro más serio consiste en que en lugar de servir como un laboratorio social en el cual otras jurisdicciones tomen lo mejor de los demás, puede darse una carrera hacia el fondo, los errores y las soluciones mínimas. En cualquier caso, dice Goodin (1996), el que las instituciones federales u otros principios de maximización de la diversidad del diseño institucional constituyan una buena idea depende, una vez más, de un juicio fundamentalmente político y social, sobre las consecuencias probables.

Entonces, Robert Goodin (1996) identifica que el diseño institucional es un proceso consensual político y social, donde pueden intervenir actores públicos y privados, nacionales e internacionales, los cuales tratarán de influir en el proceso y en el diseño para hacer valer sus intenciones, es decir sus intereses. Otra manera de entender el diseño institucional es a partir de la visión económica, la cual refiere la maximización de ganancias, el cálculo de costos y valores, preferencias y parte de supuestos como la racionalidad de los agentes, su capacidad de acción, organización e información, así como el cálculo de la anticipación, las transacciones de las preferencias y los incentivos tanto colectivos como individuales (Banks, 1995: 21).

El modelo racional del diseño institucional supone la maximización de los beneficios y la minimización de los riesgos. Esta visión parte de un proceso racional donde la información, los deseos, las preferencias y el cálculo, tanto de costos como de beneficios, pondrán restricciones y límites al diseño institucional.

Por su parte, el diseño constitucional de las instituciones incorpora en su génesis la idea de plasmar en el ordenamiento jurídico las reglas del juego. La Constitución, por lo tanto, puede integrarse con las estructuras reales de poder (La Salle, 1862), o con las normas formales que ponen límites a la discrecionalidad y proveen herramientas de estabilidad y certidumbre en el comportamiento esperado de las instituciones. Aunque también se suelen dejar espacios de discrecionalidad e incertidumbre, pues se plasman en el articulado constitucional sólo los valores generales consensuados por los diversos agentes en la discusión del diseño. De ahí la necesidad de dejar claros los intereses nacionales y generales para el Estado en la Constitución, de lo contrario la definición difusa de las instituciones en la Constitución pueden incentivar las *zonas marrones* de las que habla Guillermo O´Donnell.

En términos generales, el diseño puede ser intencional o no. Se parte de que los individuos

son los agentes de las propias instituciones; modelan su comportamiento con las propias normas que diseñan, y en ese sentido están impregnadas de intereses y pretensiones. Las instituciones definen y defienden un contexto, un parámetro de comportamiento. No son estáticas, sino dinámicas; tienen una retroalimentación interna, pero también externa; se sancionan y buscan establecerse en el tiempo en comunión con la organización que las detenta.

1.6.2 Estructura organizacional

Dice David Arellano (2000: 6-7) "que es en las organizaciones donde las acciones de los actores y grupos adquieren sentido. Donde los recursos se movilizan y se aplican. Donde las políticas se generan y luego se implementan. Donde las reglas, leyes y normas operan en la práctica". Asimismo, considera que "el gobierno es una red de organizaciones con pretensiones de actuación homogénea, lógica y continuidad", lo cual regularmente no sucede porque uno de los principios en una organización es la heterogeneidad.

Por lo tanto, las organizaciones son "espacios sociales creados en la dinámica de sociedades heterogéneas" David Arellano (2000: 11). Esto implica que las organizaciones están constituidas por personas con valores, intereses e interpretaciones que influyen en el comportamiento organizacional. De allí que las estructuras organizativas primero reconozcan que se encuentran en un entramado institucional que les provee de límites y restricciones, y que "se mueven y desarrollan a través de la acción de actores y grupos" (Arellano, 2000: 12).

La estructura organizacional que se ideó a nivel internacional para la protección de datos personales tiene la característica de ser heterogénea, aunque se ha tratado de homogeneizar optando por organizaciones públicas autónomas que se encuentren lo suficientemente alejadas de los intereses políticos centrales para que puedan cumplir con sus funciones. A estas agencias de control se les ha denominado "autoridades reguladoras o de control" (Bennett y Raab, 2003).

1.6.2.1 Autoridades de control

Una de las características de la regulación es que el Estado delega la función de garantizar las normas aplicables a órganos especializados capaces de hacer cumplir las normas y lograr impactos positivos para mitigar la conducta ilegal y negligente. En este sentido, el Estado manifiesta su actividad y voluntad a través de estos órganos, los cuales tienen las facultades para actuar ante la omisión o la manifestación de acciones en contra de las estipuladas en los ordenamientos

institucionales. Estos órganos de implementación y acción tienen un conjunto de competencias diseñadas en el aparto normativo y jurídico, incluso pueden idear otros diseños institucionales que permitan realizar sus funciones y obligaciones, de las cuales son responsables.

Estos órganos de control son, en términos de David Arellano (2000: 12), "organizaciones duales, las cuales por un lado están formal y legalmente constituidas, tanto en su existencia como en sus objetivos. Y, por otro, una vez constituidas adquieren lógica propia, se enfrentan a su propio contexto y complejidad y desarrollan capacidades y realizan esfuerzos para la sobrevivencia, como cualquier otra organización".

Independientemente de esta dualidad, deben tener la capacidad de imponer valores, normas y comportamientos específicos, así como ejercer el poder consentido por la sociedad y los agentes implicados en el diseño de las instituciones antes mencionado. El órgano es un conjunto de competencias —algo así como un cargo o una oficina— que será ejercido por una o varias personas (el funcionario público, agente o personal del Estado) que actúa dentro de las atribuciones o funciones que le han sido conferidas en el diseño institucional. Bajo este concepto se distingue entre el *órgano jurídico* (el conjunto de competencias) y el *órgano físico*, o sea, la persona o personas llamadas a ejercer esas competencias. En otra terminología, se distingue entre el *órgano-institución* y el *órgano-individuo*. Para otros autores, el órgano sería la suma de los dos elementos, el cúmulo de las funciones individualizadas y la persona llamada a ejercerlas (Bennet, 2003).

Esta clasificación de los órganos de control y protección de los datos personales permite diferenciar con mayor detalle los derechos y deberes de la persona llamada a desempeñarse como parte de las organizaciones encargadas de vigilar y proteger este derecho. Estamos frente a tres situaciones diferentes, pero concatenadas: la función del Estado, las atribuciones, responsabilidades y competencias de la organización, y el comportamiento del funcionario (el papel administrativo).

En el sistema de regulación política y económica se ha discutido sobre la autonomía de las organizaciones y su capacidad para implementar los mandatos institucionales, así como su capacidad para velar por la regulación encomendada. En el mundo se han seguido diversos modelos de organización de las autoridades de control. Desde tribunales constitucionales, tribunales administrativos, agencias de regulación dependientes de ministerios de gobierno, autoridades de control descentralizadas y las que con mayor auge han surgido en los últimos años: las autoridades autónomas de control, constitucionalmente protegidas para lograr independencia y equilibrio de poderes en la toma de decisiones (Bennet, 2003).

En las autoridades autónomas constitucionales y reconocidas como agencias de regulación independientes, se ideó su integración por personas designadas mediante procedimientos públicos de concurso de oposición y antecedentes profesionales académicos y/o de órganos imparciales e independientes, que garanticen su idoneidad técnica con prescindencia de su afiliación política, que tengan estabilidad, imparcialidad e independencia, sin intervención ni injerencia de la autoridad política de la administración central. La estabilidad, idoneidad y comunicación pública del órgano gubernamental permitirá dar estabilidad, claridad y previsibilidad de las decisiones. Estas agencias de regulación independiente, como parte de los instrumentos de regulación, se caracterizan por tener mayor independencia en sus funciones y aumento en sus actos de regulación. Aquí el Estado delega los procesos de control en la agencia (Bennet, 2003).

El auge de estas organizaciones de control autónomas ha remontado como parte de la innovación en las estructuras organizacionales del Estado, con el objetivo de brindar imparcialidad, eficacia y calidad en los servicios que ofrece (Christensen y Laegreid, 2007). El surgimiento de estas organizaciones no sólo obedece a una moda, sino a la necesidad de dar credibilidad, generar estabilidad, promover la competitividad y atender la experiencia jurídica internacional que dicta la obligación de diseñar organizaciones autónomas que protejan el derecho a la protección de datos personales, para evitar la parcialidad en la toma de decisiones.

No sólo se espera que estas autoridades sean defensoras de los derechos, sino también eduquen, auditen, capaciten, asesoren, negocien, sean intermediarios, y que sean capaces de hacer cumplir las normas, los procedimientos y proteger mediante acciones y sanciones concretas el comportamiento ilícito en el tratamiento de datos personales (Bennet y Raab 2006: 135). Entonces, las agencias de protección de datos se convierten en un nuevo intento por hacer frente a desafíos sociales que aluden a nuevas formas de interacción social entre individuos, los gobiernos y las corporaciones privadas nacionales e internacionales.

El diseño de las organizaciones también debe atender a la exigencia del contexto mediante el cumplimiento de capacidades normativas, espaciales, territoriales, de personal, recursos financieros e incluso ideológicos. Una de las herramientas que no se puede dejar de lado es la tecnología, la cual influye en la organización e impacta de manera positiva en la eficiencia de sus actividades (Margetts, 2013: 1). Nos encontramos en el contexto del gobierno electrónico y digital, el cual consiste en la integración de las funciones gubernamentales con la tecnología, haciendo frente a los nuevos retos de seguridad y de protección de derechos en la era virtual.

Las organizaciones pueden analizarse desde tres perspectivas analíticas: 1) Perspectiva

racionalista: la conducción hacia el propósito; 2) Perspectiva naturalista: diferencias, disidencias y conflictos internos y 3) Perspectiva de sistema abierto: relación con el entorno. (Arellano, 2010). Esta investigación se basa fundamentalmente en la última perspectiva, pues lo que busca es conocer la relación del entorno organizacional de la "agencia de control" sobre la protección de datos personales y su relación en el entorno con otras agencias también reconocidas como de regulación y control con su entorno administrativo y jurisdiccional.

En la protección de datos personales muchos son los elementos por considerar, pero hasta aquí se han tratado aquellos que nos permiten entender el diseño institucional y organizacional de protección de este derecho. Por ejemplo, la definición de dato personal, el fundamento y contenido del derecho a la protección de datos personales, la relación con otros derechos, el papel del Estado, el gobierno y el ejercicio de políticas públicas como acciones concretas para proteger derechos humanos; así como el diseño tanto institucional como organizacional, necesarios para la implementación de la política. En el siguiente y último apartado de este primer capítulo se sistematizará toda esta información en una categoría analítica que será la política nacional de la información a partir de la cual se integra todo el entramado teórico, analítico, metodológico y conceptual de este trabajo.

1.7 Categorías de análisis para el estudio de la protección de datos personales

Para atender problemas complejos es necesario primero conocer su origen, comprender sus vertientes y analizar las posibilidades de solución. Una manera de comprender la protección de datos personales es ajustarlo a la categoría de la política de la información, la cual comprende tres grandes políticas: la de acceso a la información y transparencia, la de protección de los datos personales y privacidad, y la de archivos, aunque no solamente se concentra en estas políticas, sino que integra políticas públicas transversales como la seguridad de la información, la videovigilancia, la ciberseguridad, el robo de identidad, entre otras.

La ventaja de considerar la política de la información como una política a nivel macro implica reconocer la necesidad multidisciplinaria del tema, la transversalidad, la coordinación, la coherencia de diversas herramientas de tipo jurídicas, económicas, tecnológicas, administrativas y sociales, todas necesarias para solucionar un problema complejo como la salvaguarda y protección de los derechos humanos fundamentales.

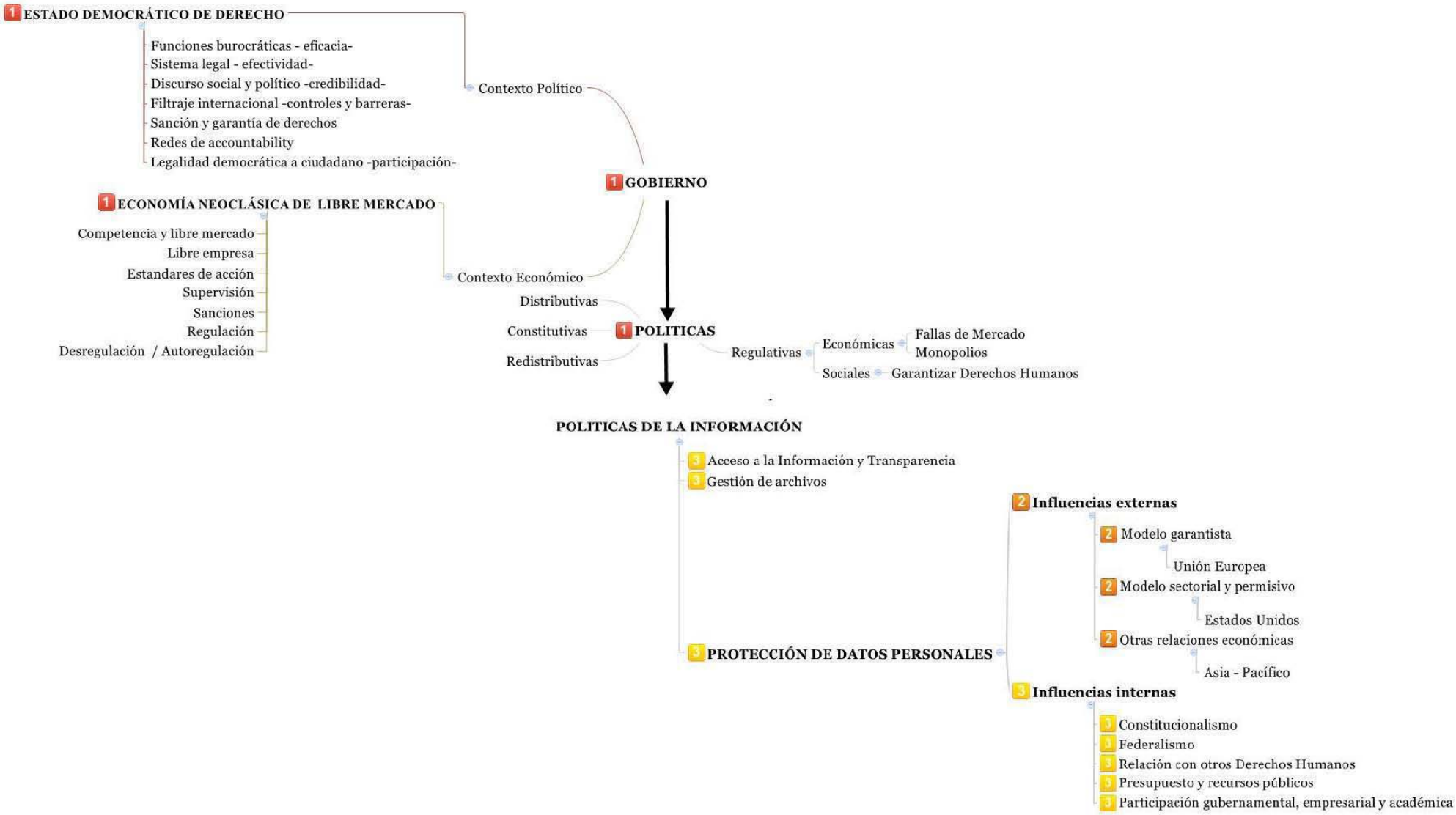
Entonces, la política de la información aparece como categoría analítica en el contexto de un

Estado democrático de derecho, el cual es promotor de los derechos humanos en todos los espacios: públicos, privados, nacionales e internacionales. La política de la información reconoce la influencia internacional, pero enfoca sus esfuerzos en la promoción de los principios nacionales en el manejo de la información en todos sus sentidos, al proveer de esquemas de seguridad, control, capacitación, información y garantía de manera coordinada y transversal, "pues cuando hay gobiernos débiles, estructuralmente corruptos y tendientes a la desorganización, la mejor propuesta es atender los problemas públicos de manera transversal" (Aguilar, 2011), que impliquen la coordinación y la totalidad del gobierno (*The whole government approach*) (Christensen y Laegreid, 2007).

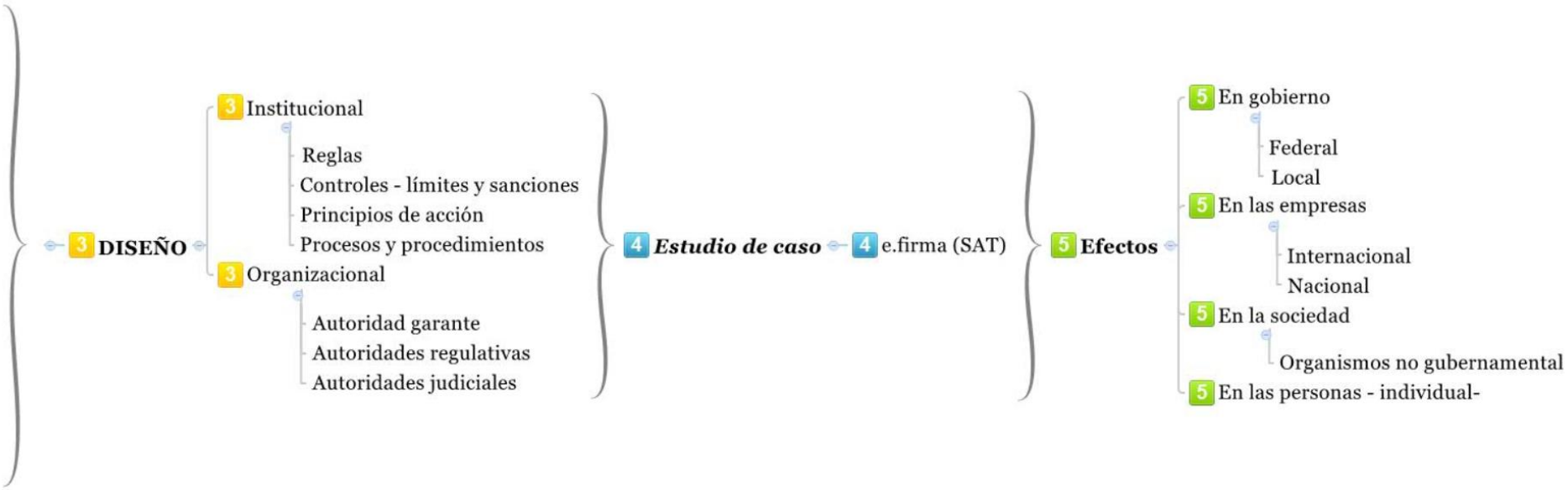
La necesidad de enfocar los esfuerzos no sólo de manera transversal, sino a partir de un enfoque de coordinación total, surge a raíz de la preocupación por el auge de la Nueva Gestión Pública, la aparición de organismos especializados, la desintegración de las funciones, la desagregación. Surge para reequilibrar el sistema atendiendo a la cooperación, la coordinación y el apoyo entre agencias de servicios para mejorar el desempeño del gobierno (Christensen y Laegreid, 2007). Con este enfoque se trabaja con una lógica de coordinación total y transversal para atender problemas complejos, que mantienen un vínculo con toda función y estructura gubernamental, como es el caso de los datos personales, tratados tanto en el sector público como en el privado. Si bien este enfoque no se encuentra totalmente afinado en sus propuestas teóricas, sí permite entender que un gobierno debe atacar los problemas complejos de manera sistemática.

En el siguiente mapa se presenta el contexto en el cual se puede visualizar la posición de las políticas de la información y todas sus interrelaciones con otros temas. En este mismo mapa se presentan los temas de estudio y el análisis de esta investigación. Todos los temas están marcados con números. Cada uno alude a los capítulos que tratan los temas allí referidos. Es, por lo tanto, un esquema sistémico de esta investigación.

Mapa 1. Estructura de la investigación por unidades de análisis y capítulos **(parte 1)**



Mapa 1. Estructura de la investigación por unidades de análisis y capítulos **(parte 2)**



Fuente: Elaboración propia. La localización numérica de los temas corresponde al capítulo de esta investigación.

Este capítulo nos permite entender que la protección de datos personales es un derecho humano fundamental diferente a la privacidad y la intimidad. Es un derecho que surge a raíz del desarrollo tecnológico y su potencial uso en el tratamiento de datos, lo que afecta de una u otra manera a las personas. Se puede entender como un derecho intermediario al proteger otros derechos o directo personalísimo cuando se protege el proceso de guarda y custodia de los datos personales. Este derecho otorga la propiedad de los datos a su titular y fomenta ciertas garantías que salvaguardan los principios, las normas y los procedimientos en el tratamiento de datos, tanto en el sector público como en el privado.

El Estado a través del gobierno y la administración pública se hace responsable de crear un sistema institucional y organizacional que concilie los diferentes intereses en torno a la protección de los datos personales, reconociendo la necesidad de utilizar la información tanto para el gobierno como para el sector privado en la provisión de bienes y servicios. Este diseño es un proceso político, económico y social que debe atender ciertos principios del diseño institucional y organizacional, a partir del propio contexto.

Para integrar soluciones acordes a la complejidad del problema en el tratamiento de los datos personales se propone sistematizar todo en *la política de la información*, una política nacional que de manera coordinada, colaborativa y transversal logre unificar criterios, principios, valores, objetivos y metas, para que de manera sistemática se atienda el problema que implica la necesidad de tratar datos, sin vulnerar los derechos y las libertades individuales.

CAPÍTULO 2. LOS MODELOS INTERNACIONALES DE PROTECCIÓN

En el mundo existen diferentes modelos institucionales y organizacionales de la protección de datos personales. Las reglas, las normas, los valores y los aparatos administrativos encargados de velar por este derecho van desde una oficina pública dependiente y jerarquizada del aparato administrativo, pasando por un tribunal judicial, hasta una organización autónoma con amplias facultades (Bennett y Raab, 2003). Estos diseños institucionales son diversos porque su desarrollo y evolución ha sido diferenciada, sin embargo, podemos encontrar dos modelos generales de protección: el garantista y el permisivo. El primero surge en Europa occidental y el segundo atiende al diseño económico y político como el de los Estados Unidos de América. Estos modelos influyeron en el diseño de la política para la protección de datos personales y resulta necesario profundizar en cada uno para lograr comprender las instituciones y organizaciones ideadas en México.

2.1 El modelo garantista europeo

El modelo europeo de protección de datos personales ha sido denominado como garantista porque provee medios de protección institucionales y organizacionales a la persona en el uso y tratamiento de sus datos personales. Estas garantías pueden entenderse a partir del discurso, los medios y los procesos para la protección de datos personales, los cuales se diseñaron considerando su experiencia, contexto y herramientas jurídicas, económicas y sociales. El diseño normativo de la Comunidad Europea se puede observar en cuatro momentos claves, de acuerdo con Mayer-Schönberger (1997: 219-241):

1. Las normas de primera generación. Aparecieron a principios de 1970 y se caracterizan por ser una reacción inicial ante el desarrollo tecnológico e informático.
2. De segunda generación. Surgen a partir de la segunda mitad de la década de 1970, y ponen énfasis en los derechos de la persona en lo individual.
3. De tercera generación. Consideradas a partir de la decisión del Tribunal Constitucional alemán sobre el censo de 1983, en donde la regulación refleja el concepto de autodeterminación informativa.
4. Las reglas de cuarta generación (consideradas "holísticas" y "sectoriales"). Modifican las imperfecciones de las normas de tercera generación y se desarrollan en un periodo donde la regulación general de protección de datos personales se complementa con

regulaciones específicas (normas para diferentes tipos de datos).

Como se puede observar los principios que fundamentan cada generación son diferentes y no excluyentes. Es un proceso de evolución acorde con las necesidades y el contexto. Mayer-Schönberger (1997: 219- 241) dice que la primera etapa de regulación inicia con la Resolución 509 de la Asamblea del Consejo de Europa sobre derechos humanos y nuevos logros científicos y técnicos. Es el primer documento que se generó sobre protección de datos personales, donde se describe cómo afecta el desarrollo tecnológico a la vida privada de las personas.

El estudio realizado por el Consejo de Europa (Resolución 509) dio a conocer que "las herramientas de desarrollo tecnológico podrían traer grandes afectaciones para las personas, ya que la normativa interna de los Estados no ofrecía las suficiente garantías para amparar la vida privada en la era cibernética y que además la Convención Europea de los Derechos del Hombre tampoco contaba con instrumentos adecuados para afrontar la tarea de proteger los bancos de datos de carácter personal ante la complejidad y amplitud de la técnica informática" (Martínez, 2016)[9] Esta situación hizo que la protección de datos se volviera un tema fundamental en la agenda pública de los países Europeos, y entonces a partir de esta resolución se sentaron las bases para legislar en la materia e idear soluciones desde el ámbito gubernamental.

Como tema central en la agenda pública de la Unión Europea y de diversos organismos internacionales, entre ellos la Organización para la Cooperación y el Desarrollo Económico (OCDE) y el Foro de Cooperación Económica Asía- Pacifico (APEC), se empezó a reconocer la necesidad de hacer una regulación uniforme en los Estados miembros de la Comunidad Europea para proteger la privacidad de los ciudadanos ante el tratamiento, informatizado o no, de sus datos. Con ello, surgen los primeros antecedentes normativos del derecho a la protección de los datos personales (PDP) en acuerdos y directrices internacionales[10] que influencian la aparición de leyes

[9] Black Edwin asegura en su libro titulado "IBM y el holocausto" que los alemanes utilizaron información de los censos de población tratada con medios tecnológicos, como lo fue la máquina Hollireng, la cual tuvo diferentes usos. Para mayores referencias consultar Black, Edwin. 2001. *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation*. United States, Crown Books.

[10] Por ejemplo: Las directrices de la OCDE relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales, 1980; Convenio número 108 del Consejo de Europa (28 de enero de 1981) para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal; Directrices de la ONU. Directrices para la regulación de los archivos de datos personales informatizados (14 de diciembre de 1990); Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos (emitida en 1995). Marco de privacidad del Foro de Cooperación Económica Asia Pacífico (APEC, 1998); Carta de los derechos fundamentales de la Unión Europea (7 de diciembre del 2000); Directrices de la comunidad Iberoamericana, relativas a armonizar la protección de datos en la comunidad Iberoamericana (2007), y Resolución en Madrid. Estándares internacionales sobre protección de datos y privacidad (Madrid, 2009).

en diversos países: Suecia en 1973; Alemania, Dinamarca, Australia, Francia, Noruega y Luxemburgo en 1978, y en los años noventa, alrededor de 20 países en el mundo optaron por legislar sobre la materia (Bennett y Raab 2003: 102-203).

En este sentido, las normas de primera generación coinciden con la aparición de los primeros sistemas de cómputo, por lo tanto, en la formulación de las primeras leyes de protección de datos sus autores tuvieron especial consideración en los desafíos de las nuevas tecnologías, para hacer su aplicación controlable y transparente. Fueron diseñadas para visibilizar la recolección masiva por parte de los Estados; proteger el derecho de acceso y rectificación, y obligar el registro de las bases de datos que contuvieran datos personales. Siendo su principal objetivo la regulación de la actividad del Estado.

La segunda fase inicia con el auge en la creación de leyes nacionales de países como Alemania, Francia, Dinamarca, Austria y Luxemburgo, así como con la Resolución del Parlamento Europeo sobre la tutela de los derechos del individuo frente al creciente progreso técnico en el sector de la informática de 1979, y culmina hasta la decisión de la Corte Constitucional de Alemania de 1983, declarando el derecho a la autodeterminación informativa (Mayer- Schönberger, 1997).

En la tercera generación, el reconocimiento del derecho a la autodeterminación informativa en Alemania es central. Viggiola y Molina (1999: 1) definen a la "autodeterminación informativa como la facultad de toda persona para ejercer control sobre la información personal que le concierne, contenida en registros públicos o privados, especialmente los almacenados mediante medios informáticos". Aquí la regulación se caracteriza por la creación de un nuevo derecho fundamental y los esfuerzos por institucionalizarlo. Este derecho es un "derecho personalísimo, de tercera generación, que ha adquirido autonomía conceptual en comparación con otros derechos de la persona como la intimidad, privacidad, la imagen, el honor, la identidad personal, y se integra en el amplio contexto de la libertad y la identidad personal".

Finalmente, se puede hablar de una cuarta generación de normas sobre protección de datos personales a partir 1995 con la Directiva 95/46/CE y termina con el nuevo reglamento 2016/679 del Parlamento Europeo y del Consejo, 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. Un aspecto relevante de esta etapa es la transferencia internacional de datos y la necesidad de armonizar legislaciones nacionales con normas internacionales. Constantemente modificadas debido a los rápidos desarrollos tecnológicos para el procesamiento de datos. Aquí el auge de leyes en todos

los continentes toma fuerza y la Unión Europea se vuelve un referente internacional en los diseños institucionales y organizacionales para la regulación en la materia. En esta cuarta etapa adquiere auge la regulación específica, es decir se amplían el tipo de datos protegidos, pero sobre todo se pretenden armonizar los niveles y estándares nacionales e internacionales a partir de los dos grandes modelos occidentales existentes.

2.1.2 Los derechos humanos ante el desarrollo de la tecnología

Estos cuatro momentos de la protección de datos personales en Europa se pueden entender a partir del discurso de los derechos humanos como un límite al desarrollo de la tecnología, como control al poder totalitario de los Estados, y no menos importante como parte del discurso del libre mercado. Lo deseable es que los derechos humanos prevalezcan sobre los intereses del Estado, de la tecnología y de las grandes corporaciones internacionales. En este sentido, el supuesto discursivo le otorga al modelo garantista la tesis proteccionista a la persona, donde el derecho humano está por encima de los poderes políticos o comerciales relacionados con los datos.

La resolución 509 del Consejo de Europa (1968) dice que es necesario proteger "en los Estados miembros los derechos humanos y libertades fundamentales reconocidos en el artículo 8[11] de la Convención sobre los Derechos Humanos, tomando en cuenta los graves peligros inherente al desarrollo moderno en ciencia, tecnología y comunicaciones, mismas que permiten con mayor agilidad la utilización no autorizada de información privada. Acciones tecnológicas que amenazan los derechos y libertades personales" (CE,1968), contra las cuales se advierte la necesidad de la acción de los gobiernos.

Estas preocupaciones entran en la agenda pública de la Comunidad Europea y de las Naciones Unidas en 1968 como resultado de una iniciativa adoptada por la Conferencia Internacional de Derechos Humanos, celebrada en Teherán, Irán, como parte del programa para el Año Internacional de los Derechos Humanos. Siguiendo las recomendaciones de esta Conferencia, la Asamblea General de las Naciones Unidas adoptó una resolución invitando al Secretario General

[11] Artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales (CEDH) del 4 de noviembre de 1950 (también conocido como Pacto de Derechos Civiles y Políticos de la ONU), dice: "1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia"; 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás"

a emprender "continuos estudios interdisciplinarios, tanto nacionales como internacional, que pudieran servir de base para la elaboración de normas adecuadas para proteger los derechos humanos y las libertades fundamentales". De aquí se derivaron las siguientes consideraciones en torno a los derechos humanos y al desarrollo tecnológico (Weeramantry, 1993):

1. El respeto a la privacidad de las personas, la integridad y la soberanía de las naciones a la luz de los avances en la grabación y otras técnicas.
2. La protección de la personalidad humana y su integridad física e intelectual a la luz de los avances de la biología, la medicina y la bioquímica.
3. Los usos de la electrónica que puedan afectar los derechos de la persona y los límites que deben colocarse sobre los usos ya existentes en una sociedad democrática; y, más generalmente:
4. El equilibrio que debe establecerse entre el progreso científico y tecnológico, y el avance integral de la humanidad.

Esta resolución acentúa los peligros que los desarrollos tecnológicos albergan con respecto a los derechos humanos y las libertades fundamentales.[12] Entonces, como problema público la protección de datos personales desde el modelo garantista aparece en 1968 como una preocupación ante la afectación del desarrollo tecnológico y por la falta de un marco normativo. Pero sólo considerar tales preocupaciones sería dejar de lado el contexto en el que se desarrolla este derecho, 1968 marca la etapa posterior a la Segunda Guerra Mundial, donde las telecomunicaciones y la capacidad de éstas para vigilar a los enemigos se potencializa durante la Guerra Fría, para identificar sus movimientos, estrategias y acciones con mayor detalle.

Es justamente el periodo intermedio de la Guerra Fría cuando el espionaje en las embajadas era una actividad común en todo el mundo, al cual eran sometidos los representantes de otras naciones. Por ejemplo, el Servicio Federal de Inteligencia alemán (BND13 informó en 1973 que diez micrófonos habían sido descubiertos en la embajada alemana en Varsovia. El doble de los descubiertos en 1972). Asimismo, desde finales de 1950 el servicio de inteligencia alemán llevaba a cabo operaciones de espionaje a misiones diplomáticas soviéticas en Bonn, tanto en las

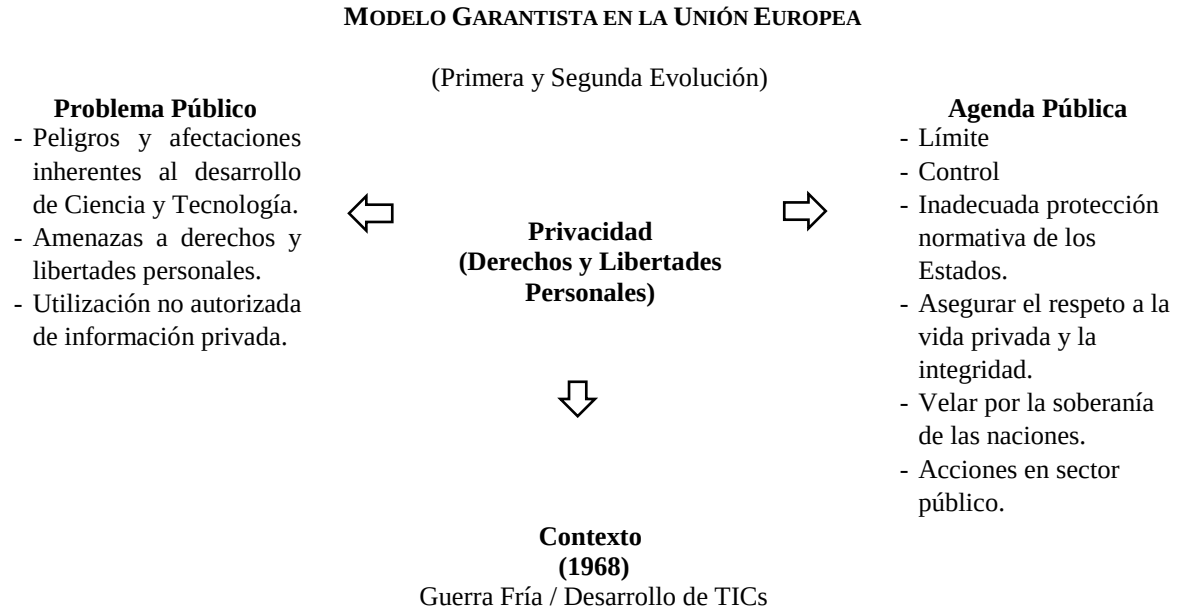
[12] Cabe aclarar, sin embargo, que en muchos casos los avances tecnológicos ofrecen oportunidades para las elecciones individuales y colectivas y para la mejora de los derechos humanos. Para profundizar en este aspecto consultar: Weeramantry, Christopher Gregory. 1990. *Human Rights and Scientific and Technological Development.* United Nations University, Tokyo, 1990.

[13] El Servicio Federal de Inteligencia (en alemán, *Bundesnachrichtendienst*, abreviado BND) es la agencia de inteligencia extranjera del gobierno alemán. Esta institución está bajo el control directo de la Oficina del Canciller.

embajadas como en los departamentos que ocupaban diplomáticos rusos en el área metropolitana de Bonn (Revenga, 2001).

De la misma manera en 1963 Patsch Werner, un empleado de la oficina federal para la protección de los derechos constitucionales (BFV),[14] reveló públicamente que algunas empresas de manera ilícita, y en conjunto con los servicios de inteligencia de los aliados, habían realizado espionaje en Alemania. Sin límites habían invadido la privacidad de los ciudadanos alemanes en teléfonos y correo personal, y que ante esta situación no se contaba con las barreras legales para detenerlos (Schmidth-Eenboom, 2001). Sólo cinco años después Europa empezó a considerar a la privacidad como un problema susceptible de entrar en la agenda pública gubernamental ante el desarrollo tecnológico. Lo antes descrito se puede esquematizar de la siguiente manera:

Esquema 5. Problemas y agenda del modelo garantista en su génesis.



Fuente: Elaboración propia.

El problema público de la privacidad en relación con el desarrollo tecnológico no sólo se puede entender a partir del discurso garantista, sino también a raíz del propio contexto. Durante la Segunda Guerra Mundial si bien el avance tecnológico era menor, en comparación con la

[14] Oficina Federal para la Protección de la Constitución, en alemán: *Bundesamt für Verfassungsschutz (BfV)*, es una agencia de inteligencia policial del Gobierno Federal alemán. Se dedica a asuntos de inteligencia e investigaciones concernientes al ámbito interno. La *BfV* responde ante el Ministerio Federal del Interior, del cual depende totalmente.

actualidad, la realidad es que las máquinas censales permitían enlistar grandes cantidades de información nacional. Edwin Black (2001) narra cómo las máquinas Hollerith utilizadas en el censo poblacional en Estados Unidos fueron utilizadas para identificar a los judíos asesinados durante el holocausto en Alemania, pero no sólo las máquinas del censo, sino también se utilizó información comercial e información migratoria. Entonces, si bien es cierto que el discurso en la primera etapa de la protección de datos se sustentó en las afectaciones del desarrollo tecnológico a las personas, el problema iba más allá: "se trataba de la soberanía de las naciones a la luz de los avances en la tecnología y sus consecuencias, ejemplo de ello el espionaje durante la Guerra Fría" (Schmidth-Eenboom, 2001: 163). Ahora se puede entender por qué el interés de las naciones por impulsar leyes nacionales de protección e incluir al individuo como base fundamental de ésta. Es sin duda una visión garantista como consecuencia de las múltiples violaciones que sufrió durante las guerras la población en Europa y las afectaciones a la privacidad de diplomáticos en todas sus jerarquías, de los gobiernos y por supuesto de las personas en general.

2.1.3 Las primeras leyes nacionales en 1970

En la década de 1970 varios países europeos adoptaron diferentes disposiciones que regularon el tratamiento automatizado de los datos. Cada uno de ellos diseñó un enfoque jurídico especial con terminología diferenciada sobre los derechos y las libertades involucrados. El Estado Federal Alemán, Suecia y Francia fueron los primeros en Europa que adoptaron preceptos jurídicos aplicables al tratamiento de la información relacionada con las personas. Estos esfuerzos constituyen un primer período que inicia en 1970 y termina en 1981 con la aprobación del Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de sus datos, documento que se convertiría en una pieza fundamental para todos los legisladores europeos, influyendo en la elaboración de las leyes posteriores (González, 2014: 56).

En 1973 y 1974, la Comisión de Ministros del Consejo de Europa adoptó dos acuerdos relativos a la protección de la intimidad de las personas frente a los bancos electrónicos de datos en los sectores privado y público, respectivamente. En ambos acuerdos se recomienda que los gobiernos de los Estados miembros del Consejo de Europa adopten medidas para dar efectividad a una serie de principios básicos de protección referidos a la obtención de datos, la calidad de estos y los derechos de las personas a ser informadas sobre su procesamiento.

También en 1977 en Viena se elaboraron una serie de principios rectores dentro de un marco general para una posible intervención internacional. En estos principios se reconocía: a) la

necesidad de una circulación de información continua e ininterrumpida entre los países, b) los legítimos intereses de los países para impedir los traslados de datos que sean peligrosos para su seguridad, o contrarios a su legislación, al orden público y la decencia, o que infrinjan los derechos de sus ciudadanos, c) el valor económico de la información y la importancia de proteger el comercio de datos mediante normas aceptadas de competencia leal, d) las necesidades de salvaguardas de seguridad para reducir al mínimo las infracciones de datos patrimoniales y el uso indebido de la información personal, y e) la relevancia de un compromiso entre los países para fijar los principios esenciales de la protección de la información personal.

Posteriormente, el Consejo de Europa, siguiendo instrucciones de su Comisión de Ministros, comenzó a elaborar un convenio internacional de protección de la intimidad sobre el tratamiento de datos en el extranjero y al transfronterizo. También inició una labor relativa a normas modelo para bancos de datos médicos y normas de conducta para los profesionales del tratamiento de datos. Asimismo, adoptó el Convenio con fecha 17 de septiembre de 1980, con el cual se establecieron principios básicos de protección de datos personales, de ejecución forzosa para los países miembro, para reducir las restricciones a la circulación transfronteriza entre las partes contratantes, y así conseguir la cooperación entre las autoridades nacionales de protección de datos y crear una comisión consultiva para la aplicación y desarrollo permanente del convenio.

2.1.4 La influencia económica en el Convenio 108 y las directrices de la OCDE

En la tercera etapa podemos ubicar la creación de las siguientes normas internacionales en materia de datos personales: las directrices de la Organización para la Cooperación y Desarrollo Económico (OCDE) relativas a la protección de la intimidad y la circulación transfronteriza de datos personales de 1980; el convenio 108 del Consejo de Europa del 28 de enero de 1981, y la declaración del Tribunal Constitucional alemán sobre el derecho a la autodeterminación informativa. En este periodo aparece un elemento analítico importante: las relaciones comerciales y el desarrollo del mercado común en Europa. Tal como lo dice Mónica Arenas (2008: 115) “los tratados constitutivos de la Comunidad Europea tenían un carácter predominantemente económico”. Carácter que en términos de datos personales se puede visualizar con las directrices de la OCDE de 1980.

Las directrices consideraron un elemento de suma importancia: “las disparidades en las legislaciones nacionales que pudieran obstaculizar la libre circulación transfronteriza de datos personales y ocasionar graves trastornos en importantes sectores de la economía, tales como la

banca y los seguros", en este sentido ellos consideran la circulación transfronteriza de datos personales como un elemento inminentemente económico, que "contribuye al desarrollo económico y social", por lo que su propuesta fue delinear un conjunto de principios para que sus países miembros pudieran incorporar esta regulación en sus legislaciones y evitar "la circulación transfronteriza de datos personales" y evitar obstáculos a la economía internacional (OCDE, 1980), y con ello "fomentar la libre circulación de información entre los países miembro y a evitar la creación de obstáculos injustificados al desarrollo de las relaciones económicas y sociales entre los países miembro", así como promover "el derecho a la libre empresa" (José Luis Piñar, entrevista personal, 2014).

Al igual que las directrices de la OCDE, el convenio 108 del Consejo de Europa del 28 de enero de 1981 tuvieron como primera preocupación el respeto a las personas de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal, no importando su nacionalidad o su residencia. A partir de este convenio se instituye el día 28 de enero como el "día de la protección de datos" a nivel internacional. Pero también en el convenio 108 se reconoce la preocupación por el flujo transfronterizo de datos, la adhesión de los principios tales como: a) la calidad de datos; b) el compromiso de las partes; c) la seguridad de datos; d) ciertas excepciones y restricciones; e) sanciones; f) necesidad de contar con una autoridad designada para la protección de los datos; g) derecho y práctica administrativa; h) petición de asistencia y ayuda mutua, y finalmente promover una protección más amplia (CE, 1981).

También se reconoció que la protección de la intimidad y de las libertades individuales adoptada por los diversos países poseen muchas particularidades en común. Así, es posible identificar ciertos intereses o valores básicos que se consideran componentes elementales de la esfera de protección. Algunos principios esenciales de este orden son: fijar límites a la recolección de datos personales, de acuerdo con los objetivos de quien los recoge; la restricción al uso de datos para ajustarse a finalidades especificadas con claridad; crear servicios para que las personas se enteren de la existencia y el contenido de los datos, dar la posibilidad de corrección, y la identificación de las partes que sean responsables del cumplimiento de las normas y decisiones de protección. En lo general, con estas normas se trató de proteger la intimidad y las libertades individuales a partir de regular el tratamiento de datos, que inicia con la recolección y finaliza con la supresión u otra medida análoga. Permitiendo la información, participación y el control por parte del individuo.

El aspecto económico de la protección de datos en este periodo se observa con las directrices de la OCDE y con el convenio 108. El contexto en esta etapa también nos provee de ciertos elementos de análisis. En 1980 Ronald Reagan, como presidente electo de los Estados Unidos de América (EUA), planteó como remedio a la crisis del Estado de Bienestar, la vuelta a las reglas de mercado, suprimiendo o flexibilizando toda normativa que pusiera obstáculos a la economía. Una política liberal idéntica es la que aplicó Margaret Thatcher en el Reino Unido desde su victoria en 1979. Oponiéndose al consenso establecido desde 1945, exaltando el esfuerzo individual y esperando de las prácticas liberales un enderezamiento de la economía británica, según ella deteriorada por el intervencionismo estatal (Harvey, 2005: 39-40). Si bien los atributos económicos de la protección de datos personales se iban configurando en este contexto y bajo estas directrices y consensos, la resolución del Tribunal Constitucional Alemán, del 15 de diciembre de 1983 donde se declara inconstitucional la Ley del Censo de Población, constituyó el antecedente en la elaboración del derecho conocido en Alemania como "la autodeterminación informativa". Este derecho va a impregnar –a la protección de datos– una de las características más importantes: la acción y responsabilidad del individuo sobre sus datos personales. Si bien en el texto constitucional alemán no se contempla el reconocimiento de un derecho a la protección de datos, menos aún a la informática, si encuadra la protección general de la personalidad, vinculado a la dignidad humana señalada en los artículos 1[15] y 2[16] (García, 2007).

Así, el derecho a la autodeterminación informativa" tuvo como fundamento lo establecido en los artículos 1 (apartado1) y 2 (apartado 1 y 2) de la Ley Fundamental Alemana, por lo que sería considerado como una concreción jurídica fundamental del derecho común de la personalidad, el cual haría frente a los cambios tecnológicos que ya presentaban una amenaza para la personalidad (García, 2007: 4). Por lo que el tribunal, partiendo del derecho general de la personalidad, señaló que "en el ordenamiento de la Ley Fundamental de Bonn se encuentran el valor y la dignidad de la persona, que actúa con libre autodeterminación como miembro de una sociedad libre. "De ahí que le sea dado a cada sujeto el poder de decisión sobre cuándo y dentro

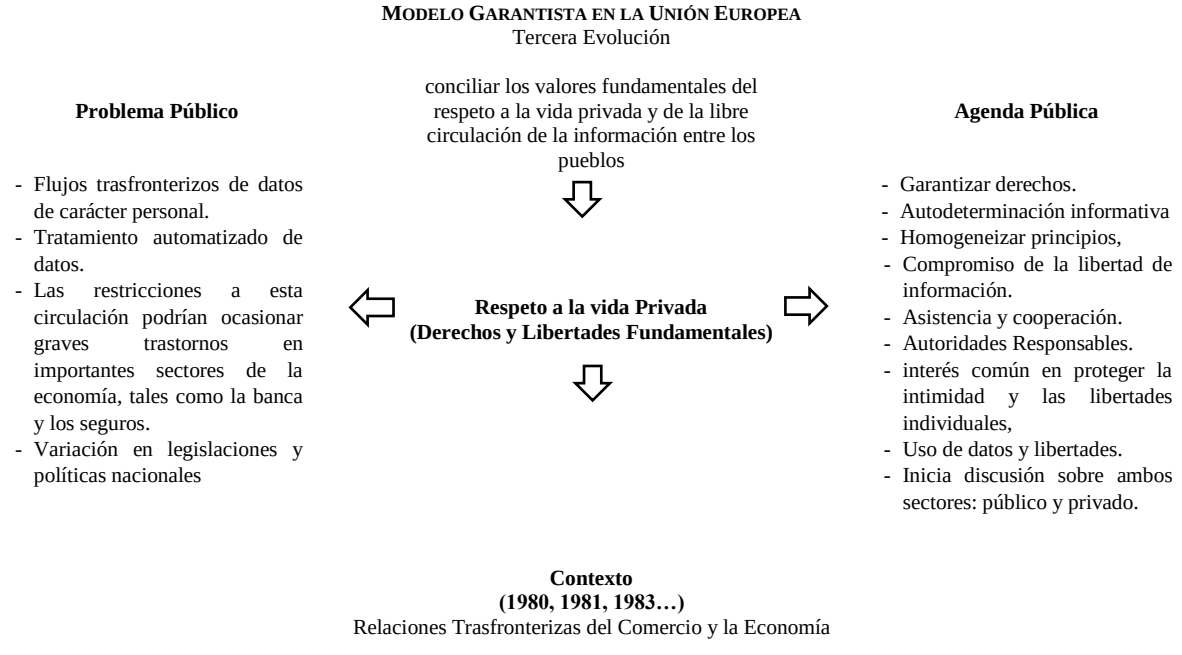
[15] Artículo 1. Sobre la protección de la dignidad humana, vinculación de los poderes públicos a los derechos fundamentales, y que en su consecutivo 1.1. sostiene que: "La dignidad humana es intangible. Respetarla y protegerla es obligación de todo poder público". *Ley Fundamental de la República Federal de Alemania*, 23 de mayo de 1949. Disponible en: https://www.btg-bestellservice.de/pdf/80206000.pdf

[16] Artículo 2. Sobre la Libertad de acción y de la persona, que en su consecutivo (1) declara: "Toda persona tiene el derecho al libre desarrollo de su personalidad siempre que no viole los derechos de otros ni atente contra el orden constitucional o la ley moral", y (2) Toda persona tiene el derecho a la vida y a la integridad física. La libertad de la persona es inviolable. Estos derechos sólo podrán ser restringidos en virtud de una ley. *Ley Fundamental de la República Federal de Alemania*, 23 de mayo de 1949. Disponible en: https://www.btg-bestellservice.de/pdf/80206000.pdf

de qué límites considera revelar situaciones y aspectos de su propia vida. Pues es precisamente en esa "autodeterminación consciente y responsable" del sujeto donde radica el derecho fundamental a la protección de datos de carácter personal (Del Castillo, 2007: 138).

De ahí que este derecho, en tanto que fundamental, se constituya en garantías subjetivas de la esfera más allegada al sujeto, a la persona. Garantías que operan, incluso, frente al legislador, a quien únicamente le será dada la posibilidad de configurar la eficiencia material, organizativa y procedimental de los derechos. Lo que para la protección de datos personales como derecho fundamental conlleva una gran responsabilidad individual de la cual las personas deben hacerse conscientes. Esta tercera evolución de la protección de datos personales se puede resumir en el siguiente esquema, en donde se identifican los principales elementos que permiten definir la acción gubernamental en torno al manejo de datos personales en Europa a partir de 1980 y hasta la promulgación de la directiva 96 del Consejo de Europa.

Esquema 6. Problema y agenda del modelo garantista en su desarrollo intermedio.



Fuente: elaboración propia.

Resulta importante resaltar en esta etapa que estas directrices y lineamientos internacionales están considerando a los datos personales como una herramienta para proteger los derechos y las libertades fundamentales, así como la intimidad y la privacidad de las personas. De esta manera,

se empieza a constituir la protección de datos personales como parte fundamental de la protección de otros derechos de mayor amplitud: la privacidad, la intimidad y las libertades individuales. Con la configuración de la autodeterminación informativa alemana. La protección de datos personales adquiere una de sus características vinculadas al contexto económico preponderante y a los principios de directrices y lineamientos internacionales: el uso de datos legítimo bajo el consentimiento de la persona y la responsabilidad de ejercer y exigir este derecho. Se le adjudica a la persona la responsabilidad de *sí mismo*, una gran responsabilidad donde el derecho subjetivo le otorga la capacidad de acción.

Por lo tanto, la tercera etapa edificó un sistema relativo a la elaboración y conservación de los datos a través de distintas normas de carácter general sobre la base del principio de la libre autodeterminación informativa. Estas aportaciones fueron renovadas en una cuarta etapa de la regulación relativa a la protección de datos personales, donde entró en vigor la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, del 24 de octubre de 1995; el marco de Privacidad del Foro de Cooperación Económica Asia Pacífico (APEC, 1998); las directrices de la comunidad iberoamericana, relativas a armonizar la protección de datos en la comunidad iberoamericana (2007) y la resolución de Madrid: Estándares internacionales sobre protección de datos y privacidad (Madrid, 209). En el siguiente apartado se analiza esta etapa.

2.1.5 Directiva del Consejo de Europa y diseño actual

La Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, tiene los siguientes elementos particulares:

1. "El principio de lealtad y buena fe en la licitud y corrección de la gestión y elaboración automática de datos.
2. El principio de legalidad en la legitimidad y determinación anticipada de las finalidades, motivos y causas de la inscripción de los datos.
3. La utilización de los datos gestionados y elaborados de conformidad con las finalidades predeterminadas.
4. Posibilidad de los intereses de modificar, extinguir y actualizar los datos y que sean acordes a la realidad.
5. La conservación de los datos durante un tiempo suficiente para lograr las finalidades

para las cuales fueron registrados y elaborados" (CE, 1995)

El convenio tuvo algunas modificaciones en 1991 por parte del Comité Económico y Social (1991) y del Parlamento (1992) con la pretensión constante de fortalecer el principio de consentimiento del afectado para el tratamiento de los datos de carácter personal, dentro del marco del respeto a la vida privada y de la identidad del sujeto. Todo planteamiento del tema parte de que el dato de carácter personal no es propiedad de quien lo posee o maneja, sino de su titular o persona a quien concierne el dato, por lo que la salvaguarda de la personalidad exige la adopción de medidas tendientes a frenar el uso de terceros y los límites fundados en el derecho, lo que se traduce en la regulación segura de los flujos transfronterizos de datos, como elemento necesario para el desarrollo del comercio internacional y el fortalecimiento de la cooperación científica y técnica. De modo que además de la protección de la vida privada de las personas, la Directiva considera la protección de intereses estatales relativos al control de la información de las personas, más allá de las fronteras europeas, impidiendo, en muchos casos, la salida de datos de la jurisdicción comunitaria.

El tipo de protección que vela por el manejo de datos de la población de una nación, más allá de sus propias fronteras, se puede fundamentar en la seguridad pública, la defensa, la seguridad del Estado, considerando a los datos como patrimonio de una cultura (Conde, 2005: 55, citado por Del Castillo, 2007: 99), y de una nación soberana específica. De esta manera, si las naciones tienen políticas públicas para velar por el patrimonio, entonces hay suficientes motivos para que exista una política nacional para la protección de datos personales.

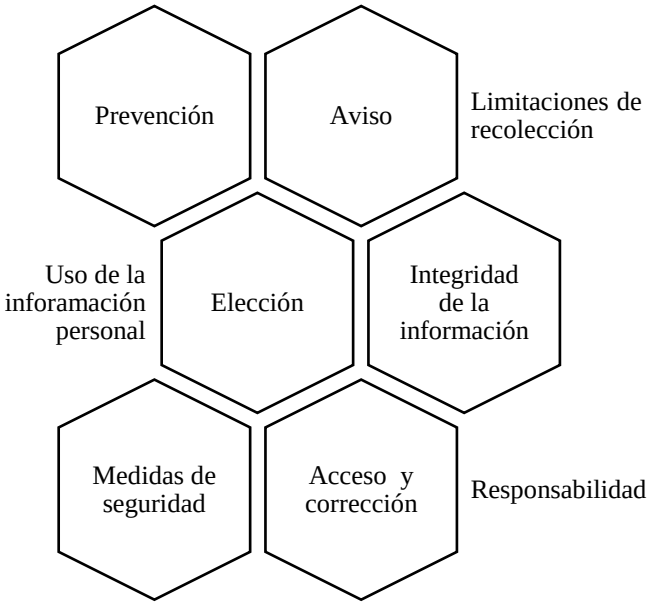
La Directiva del CE de 1995 en su artículo 28 "introduce las medidas capaces de garantizar un nivel mínimo de protección, para lo cual ordena a cada Estado miembro la disposición de una o más autoridades públicas de control, que actuarán como verdaderas guardianas de los países miembro, que estarán encargadas de vigilar la aplicación en su territorio de las disposiciones adoptadas", por lo que se propone crear organizaciones para la protección de este derecho que sean de carácter consultivo o independiente.

También ordena la elaboración de códigos de conducta, destinados a contribuir en la función de los particulares de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la Directiva, y contempla los procedimientos destinados a la prevención y solución de diferencias, con sanciones previsibles que establecerán los Estados en caso de incumplimiento de las disposiciones adoptadas en su ejecución. Establece las condiciones generales para la licitud del tratamiento de datos de carácter personal, con la

consolidación de los principios de la calidad de datos, de la legitimidad del tratamiento, la información del interesado, el derecho de acceso del interesado a los datos, el derecho de oposición del interesado, la confidencialidad y seguridad del tratamiento y la consignación de los recursos judiciales, responsabilidad y sanciones aplicables a quienes vulneren las disposiciones dictadas para la protección del derecho (CE, 1995)

De la misma manera, el marco de privacidad del Foro de Cooperación Económica Asia Pacífico (APEC, por sus siglas en ingles) y sus economías miembros, reconocen la importancia de proteger la privacidad de la información y mantener los flujos de información entre economías de la región y entre sus socios comerciales. Este marco surge a raíz de la aprobación del programa para la acción en el comercio electrónico de 1998, que pretende la cooperación para lograr beneficios comunes entre gobiernos y empresas, sin afectar a los individuos y otorgándoles beneficios como consumidores. Siendo uno de sus objetivos "mejorar los marcos de privacidad para llegar a la confianza del consumidor y asegurar el crecimiento del comercio electrónico, buscando la cooperación balanceada para proteger la privacidad y asegurar el libre flujo de información en la región Asia Pacífico" (APEC, 1998). Los principios que promueve el marco de privacidad APEC son los siguientes:

Esquema 7. Principios que promueve el marco de la privacidad APEC.



Fuente: Elaboración propia con datos de marco de privacidad APEC, 1998.

Es importante ubicar este marco de privacidad como los lineamientos que pretenden proporcionar cierta orientación y dirección a empresas dentro del contexto económico de APEC, sobre asuntos

comunes de privacidad y su impacto en los negocios legítimos, y lo hace destacando las expectativas razonables del consumidor moderno de que las empresas reconocerán sus intereses de privacidad de forma consistente con los principios promovidos en este marco, se trata de balancear la privacidad de la información con las necesidades empresariales y los intereses comerciales, y al mismo tiempo concede el debido reconocimiento a las diversidades culturales y económicas" con el fin de desarrollar parámetros para la información personal, contra las intrusiones no deseadas y el uso incorrecto de la información personal, y reconocer el libre flujo de información como algo esencial para economías de mercado desarrolladas y en desarrollo (APEC, 1998).

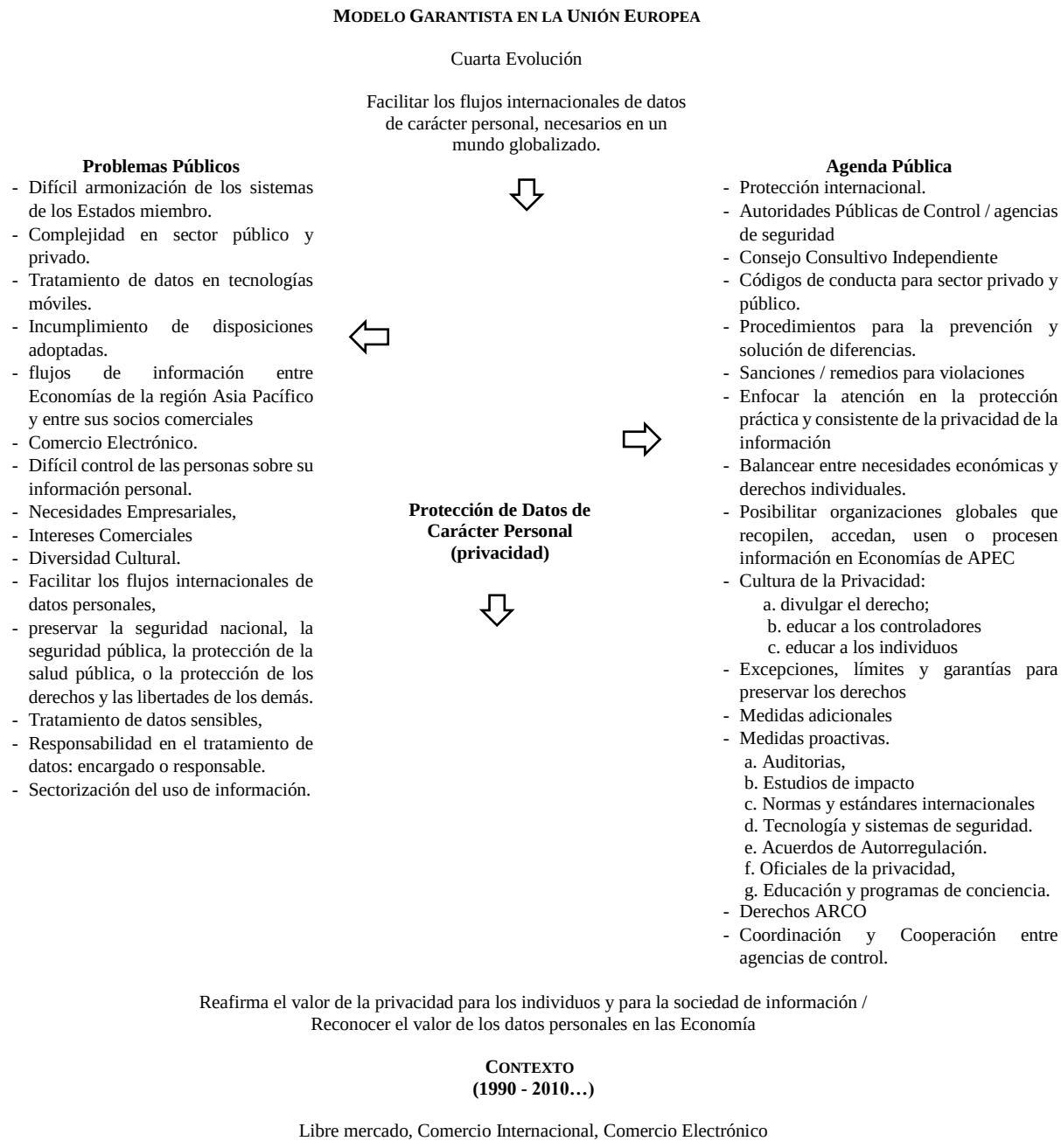
Por su parte, la resolución de Madrid (2009) fue el resultado de los acuerdos de casi cincuenta países, bajo la coordinación de la Agencia Española de Protección de Datos y trató de plasmar los múltiples enfoques que admiten la protección de este derecho, integrando legislaciones de los cinco continentes. Su carácter consensuado aportó dos valores añadidos esencialmente novedosos. Por un lado, enfatiza la vocación universal de los principios y garantías que configuran este derecho; del otro, reafirma la factibilidad de avanzar hacia un documento internacionalmente vinculante que contribuya a una mayor protección de los derechos y libertades individuales en un mundo globalizado, y por ello, caracterizado por las transferencias internacionales de información. Desde ese momento, las autoridades de supervisión y control de la privacidad asumieron la exigente tarea de difundir y promover el firme compromiso de garantizar a sus ciudadanos una mejor protección de la privacidad y de los datos de carácter personal.[17]

El 27 de abril de 2016 se promulgo el Reglamento Europeo 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos, y por el que se deroga la Directiva 95/46/CE (CE, 2016). Este reglamento provee a la Comunidad Europea un marco general de regulación del derecho a la protección de los datos personales, e influye a nivel mundial posicionándose como uno de los avances más garantistas de este derecho.

El siguiente esquema resume los aspectos más importantes del modelo garantista europeo revisado con anterioridad.

[17] Estos cambios han sido fundamentales como modelos a nivel internacional. En México sin duda ha tenido incidencia, sin embargo, dado el periodo analítico, queda fuera del análisis de esta investigación, lo que no implica dejar de reconocer su influencia para investigaciones futuras definidas en las conclusiones. Es decir, esta investigación contempla el análisis hasta 2015, por lo que los acontecimientos posteriores se tratan como parte de las conclusiones y de las investigaciones futuras sobre el tema.

Esquema 8. Problemas y agenda del modelo garantista para el diseño actual.



Fuente: Elaboración propia, a partir del contexto y la regulación de Europa de 1990

En la cuarta etapa, la regulación relativa a la protección es importante para entender cómo se ha ido modificando, pero a la vez manteniendo el discurso garantista de la Comunidad Europea con respecto tratamiento de los datos personales. El Convenio 108, la directiva 95/46/CE del Parlamento Europeo, el marco de privacidad APEC y la resolución de Madrid, son estándares internacionales sobre protección de datos y privacidad (Madrid 209), los cuales coinciden y

convergen en los siguientes principios (valores) e intereses.

Cuadro 2. Principios para la protección de datos personales.

Principio / Deber	**Convenio N. 108**	**Directiva 95/46/CE**	**Resolución de Madrid**	**Marco de Privacidad APEC**
Licitud	√	√	√	√
Consentimiento	**X**	√	√	√
Información	√	√	√	√
Calidad	√	√	√	√
Finalidad	√	√	√	√
Lealtad	√	√	√	√
Proporcionalidad	√	√	√	√
Responsabilidad	**X**	**X**	√	√

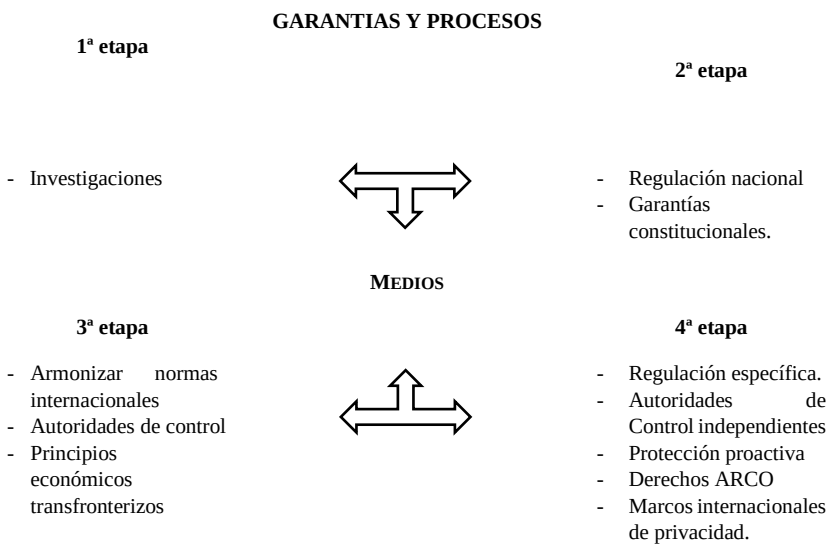
Fuente: Elaboración propia con información de la Lina Ornelas, 2013.

En resumen, el uso de información de las personas a partir de 1969 fue considerado como un problema público e ingresó a la agenda pública, volviéndose un tema central con las primeras leyes nacionales de "Suecia en 1973; Alemania, Dinamarca, Australia, Francia, Noruega y Luxemburgo en 1978" (Bennett y Raab 2003: 102-203), y justo el núcleo central de estas primeras legislaciones fue velar por su soberanía otorgando derechos y garantías para proteger la privacidad de las personas de "los peligros inherentes al desarrollo de la Ciencia y la Tecnología" (resolución 509, 1968), específicamente de los avances en la grabación y otras técnicas de comunicación. Entonces las etapas muestran que primero se reconoció el problema y se realizaron diagnósticos a partir de investigaciones diversas; luego se impusieron las primeras normas generales, y lo consecuente fueron las normas específicas nacionales y el diseño de las organizaciones de la administración del Estado para controlar y vigilar este nuevo derecho humano.

A partir de estos avances el tema de la protección de los datos se vuelve estratégico en la agenda pública de la Unión Europea y de diversos organismos internacionales como la Organización para la Cooperación y el Desarrollo Económico (OCDE) y el Foro de Cooperación Económica Asía-Pacifico (APEC), por las implicaciones económicas. Se reconoce, entonces, la necesidad de hacer una regulación uniforme en los Estados miembros de la Comunidad Europea para proteger la privacidad de los ciudadanos ante el tratamiento, informatizado o no, de sus datos. Con ello, surge el derecho a la protección de los datos en acuerdos y directrices internacionales

que influencian la aparición de leyes en diversos países, y en los años 90 alrededor de 20 países en el mundo optaron por legislar sobre la materia (Bennett y Raab 2003: 102-203).

Esquema 9. Acciones para la protección de datos en la Unión Europea.



Fuente: Elaboración propia.

En este sentido, el modelo de la Unión Europea combina opciones de solución. Primero provee a las personas de seguridad jurídica nacional, con un sistema de normas generales que garantizan ciertos valores nacionales y principios constitucionales, enmarcados en los derechos humanos fundamentales; luego crea y promueve autoridades, principalmente autónomas, que vigilen y garanticen la protección de este derecho. Las herramientas provistas se ampliaron para el sector privado, con la necesidad de extender la regulación específica y sectorial. Es importante mencionar que el modelo sectorial está definido por economías más abiertas como la de Estados Unidos de América.

2.2 Modelo sectorial de los Estados Unidos de América

El derecho a la privacidad en los Estados Unidos de América (EUA) tiene como origen la idea de libertad inherente a la cultura política, social y económica de los EUA. De esta manera, más que salvaguardar el derecho a la protección de datos personales, se protege la privacidad, a partir de considerarla como una extensión de la libertad. Tal como lo definimos en la teoría sobre el Estado

Liberal de Derecho. Este hecho implica diseños institucionales y organizacionales diferentes a los ideados y diseñados para la Unión Europea.

La privacidad para ellos es un derecho de máxima importancia, cuando la protección de datos personales es más bien una herramienta que les permite, principalmente a particulares (empresas y corporaciones nacionales e internacionales) velar por la seguridad de los datos que tienen en su posesión. Es una herramienta de protección para las relaciones comerciales nacionales e internacionales. De allí que el derecho a la privacidad se haya definido a partir de casos específicos que le fueron dando su contenido y fundamento. Estas decisiones fueron a partir de casos y juicios llevados a la Corte Suprema de Justicia, donde ésta emitió sus resoluciones acotando un espacio determinado de libertad para los ciudadanos de EUA. Veamos cómo se construye e idea este diseño.

2.2.1 Los casos judiciales como génesis

Si bien la libertad es un principio en la estructura institucional de los EUA, el derecho a la privacidad como tal, dice Carlos Gregorio (2006), estuvo más bien constituido por precedentes judiciales ante la Corte Suprema de Justicia. Dentro de los primeros precedentes se encuentran casos como los siguientes.

1. *"Meyer vs. Nebraska* (262/US, 1923) y *Pierce vs. Society of Sisters,* donde la Corte Suprema de Estados Unidos declara inconstitucionales las leyes estatales que iban demasiado lejos en el adoctrinamiento de niños, mostrando la analogía con la práctica que existía en Esparta al encerrar a los niños varones en barracas a la edad de siete años para adoctrinamiento estatal.
2. Caso *Pierce vs. Society of Sisters* (268/US, 1925), el cual ataca una ley que hacía obligatoria la enseñanza inicial en inglés.
3. El caso *Skinner vs. Oklahoma* (316/US/535, 1942) deja sin efecto una ley que establecía la esterilización de ciertos criminales.
4. *Y en Griswold vs. Connecticut* (381/US/479, 1965) se ataca una ley en la que se prohibía el uso de anticonceptivos. En este caso es donde la Corte comienza a llamarlo "derecho de privacidad" (Gregorio, 2006).

Estos casos muestran por lo menos dos cosas: el reconocimiento de que el Estado tiene poder, pero que éste puede ser excesivo y que por lo tanto se debe limitar su actuación para asegurar un espacio

de libertad a las personas. De aquí en adelante las principales sentencias de la Corte Suprema relacionadas con la intimidad han estado vinculadas a temas de sexualidad y la preservación de su intimidad. De esta manera, el concepto de privacidad transitó después a situaciones mucho más controvertidas:

1. Como en el caso *Cruzan vs. Director, Missouri Department of Health* (497/US/261, 1990) por rehusarse a tratamiento médico,
2. *Roe vs. Wade* (410/US/113, 1973) por aborto, y
3. *Washington vs. Glucksberg* (521/US/702, 1997) por suicidio asistido (Gregorio, 2006).

La mayor peculiaridad de los casos judiciales en EUA que construyeron el derecho a la privacidad es que predominantemente se focalizaron en la sexualidad (en sentido amplio, o sea decisiones y conductas relacionadas con las condiciones bajo las cuales el sexo es permisible), las instituciones sociales alrededor de las relaciones sexuales, y las consecuencias procreativas del sexo. Considerando tal situación, dice Carlos Gregorio (2006) que los pioneros de la privacidad no fueron Samuel D. Warren y Louis D. Brandeis, sino Sigmund Freud, pues en su visión de la sexualidad ocupa un estrato psicológico y biológico en la formación de la identidad y, al mismo tiempo, determina el límite interior del área estrictamente personal que el Estado no debe atravesar. Quizás el salto más interesante en la creación de motores de búsqueda fue también desarrollado por Freud, pues el psicoanálisis puede ser visto en realidad como un motor de búsqueda que permite indagar una parte de la memoria.

Jed Rubenfeld (1989) dice que las decisiones de la Corte Suprema conciben a la privacidad más bien como un conjunto de limitaciones de un Estado totalitario. En este sentido cita el caso *Loving vs. Virginia* (388/US/1, 1967) de un matrimonio interracial donde el tema de fondo no es —como el fallo declara—si una persona tiene derecho a casarse con quien quiera, lo que se discute es si el Estado tiene el derecho a intentar mantener la raza pura. También cita la opinión del juez Jackson en *West Virginia State Board of Education vs. Barnette* (319/US/624, 1943), cuando, en medio de la Segunda Guerra Mundial, declara inconstitucional una ley que obligaba a los niños escolares a saludar a la bandera y profesar fidelidad a su país (Rubenfeld, 1989).

Un caso que será importante para el tema de la privacidad en los Estados Unidos es el de *Whalen vs. Ro*e, donde se reconoce el conflicto entre el interés individual para impedir que se difundan datos personales y el interés de disponer de información para tomar cierto tipo de decisiones importantes (429/US/589, 1977). En este caso se cuestiona una ley del Estado de Nueva

York que creaba un registro centralizado y computarizado para mantener las prescripciones médicas con información completa que permitía identificar al paciente. La Corte estableció que el derecho a recolectar y usar tal información para propósitos públicos está acompañado por la obligación de impedir cualquier diseminación (propagación) sin garantías. Entonces se reconoce la necesidad pública de crear bases de datos, pero a partir de garantías definidas y respetadas por las estructuras administrativas y de gobierno. Tradicionalmente, el derecho a la privacidad ha sido relacionado con la decimocuarta Enmienda que dice:

> "Todas las personas nacidas o naturalizadas en los Estados Unidos y sometidas a su jurisdicción son ciudadanos de los Estados Unidos y de los Estados en que residen. Ningún Estado podrá dictar ni dar efecto a cualquier ley que limite los privilegios o inmunidades de los ciudadanos de los Estados Unidos; tampoco podrá Estado alguno privar a cualquier persona de la vida, la libertad o la propiedad sin el debido proceso legal; ni negar a cualquier persona que se encuentre dentro de sus límites jurisdiccionales la protección de las leyes, igual para todos" (*Bill of Rights*, XIV Enmienda, 1971).

También con la IV Enmienda se reconocen las garantías de búsqueda y aprehensión, considerando que es:

> "El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas" (*Bill of Rights*, IV Enmienda, 1971).

Esta IV Enmienda dice que para realizar registros e incautaciones es necesaria una orden de registro. También se puede fundar y motivar a partir de la I Enmienda y de la V:

> "I Enmienda. El Congreso no hará ley alguna por la que adopte una religión como oficial del Estado o se prohíba practicarla libremente, o que coarte la libertad de palabra o de imprenta, o el derecho del pueblo para reunirse pacíficamente y para pedir al gobierno la reparación de agravios.
>
> "V Enmienda. Nadie estará obligado a responder de un delito castigado con la pena capital o con otra infamante si un gran jurado no lo denuncia o acusa, a excepción de los casos

> que se presenten en las fuerzas de mar o tierra o en la milicia nacional cuando se encuentre en servicio efectivo en tiempo de guerra o peligro público; tampoco se pondrá a persona alguna dos veces en peligro de perder la vida o algún miembro con motivo del mismo delito; ni se le obligará a declarar contra sí misma en ningún juicio criminal; ni se le privará de la vida, la libertad o la propiedad sin el debido proceso legal; ni se ocupará la propiedad privada para uso público sin una justa indemnización" (*Bill of Rights*, IV Enmienda, 1971).

Lo que reconocen estas Enmiendas en torno al derecho a la privacidad es el derecho que tienen las personas y el pueblo de los EUA a estar primero bajo resguardo de la legalidad, los derechos y las normas; luego a limitar el poder del Estado y asegurar un espacio de libertad de ser y hacer. Como podemos observar, "este derecho se ha convertido en la libertad personal protegida por la 14ª enmienda, así como por las enmiendas 1ª, 4ª y 5ª, que también brindan cierto tipo de protección" (Cornell University Law School, 2016). Aunque en este modelo si bien existen principios generales como la libertad, la realidad es que cada caso se construye con sus particularidades.

El derecho a la privacidad se ha constituido de manera diferenciada al derecho que limita el acceso a la información personal. Son por lo tanto dos derechos que se diferencia en su contexto y contenido. En este sentido se reconoce que el derecho a la privacidad ha evolucionado para proteger la capacidad de las personas para determinar qué tipo de información sobre sí mismos se recopila, y cómo se utiliza esa información. Este tipo de situaciones surge, tal como lo hemos narrado en esta investigación, cuando se recopila información en sitios privados, como los sitios web con las *cookies* o en otras empresas nacionales o internacionales con fines publicitarios y comerciales" (Cornell, 2015). En el siguiente apartado se profundizará en esta evaluación del derecho a la privacidad en los Estados Unidos.

Hasta aquí, resulta importante resaltar que el modelo americano de privacidad descansa sobre la fuerza de la ley, en la capacidad de las normas, en los principios nacionales y en las decisiones judiciales para limitar las acciones de un Estado que pudiera resultar invasor y totalitario. Esta construcción de la privacidad es una limitación sucesiva para impedir que leyes —dictadas dentro de los procedimientos constitucionales— terminen asignando al Estado poderes excesivos.

2.2.2 Uso y tratamiento de la información personal. *The Privacy Act*

El derecho a la privacidad en los Estados Unidos de América si bien se funda en la libertad y la

posibilidad de tener unos espacios libres de intervención del Estado, también ha evolucionado, llegando a la posición donde se desprende el derecho de la persona a regular el uso y tratamiento de su información personal. Es decir, aquí ya se está partiendo de que en origen este uso y tratamiento existe, pero que debe ser utilizado y tratado con base en ciertos principios, lineamientos y acuerdos normativos establecidos. Aquí está bien definido lo que hoy se conoce como "derecho a la protección de datos personales" que es un derecho diferente al de la privacidad, ligado y cercano, pero diferente. Es, como dicen en Estados Unidos, una evaluación o una extensión del derecho a la privacidad (E. Igo, 2018)

Por ejemplo, Wilma Arellano Toledo y Ana María Ochoa Villicana (2012) hacen una distinción entre derecho a la información, a la privacidad y los derechos de autor, de la siguiente manera: Se centran en el tipo de intereses que persigue cada derecho. Dice por ejemplo que mientras que el derecho de autor protege los derechos de propiedad de un titular sobre su trabajo, los derechos de privacidad y publicidad protegen los intereses personales presentes en o por el trabajo. Entonces, la publicidad y la privacidad aparecerán cuando se hace uso comercial de los escritos de una persona, de la grabación de su voz, fotos u otras imágenes de ellos. Entre otras situaciones donde se invada de manera irrazonable el derecho de una persona a estar sola cuando se apropien de su nombre, cuando se publiquen asuntos. De allí que en los EUA hayan recurrido "regularmente a la privacidad para hablar de cosas tan diferentes como las relaciones íntimas, los espacios de vida, los datos personales, los derechos políticos e incluso sobre la psique. Es una definición de privacidad que la propia evolución le impregna el principio de flexibilidad" (E. Igo, 2018: 7). Por lo tanto, en los Estados Unidos no se contemplan leyes generales que concentren la protección de datos personales. Por el contrario, existe un conjunto diverso de leyes específicas que regulan la privacidad de las informaciones personales.

2.2.3 Leyes sectoriales

La legislación específica en EUA se define a partir de sectores determinados, siendo algunos los siguientes:

- Ley de Informes crediticios (*Fair Credit Reporting Act, Public Law* 91-508, modificada varias veces entre 1996 y 2001);
- Ley de archivos de televisión por cable (*Cable Communications Policy Act*, 47 USC 521-611, 1994);

- Ley de comunicaciones electrónicas (*Electronic Communications Privacy Act*, de 1986, 18 USC 2510-2520, 1994 & Supp.1997);
- Ley sobre comunicaciones en una investigación criminal (*Omnibus Safe Streets and Crime Control Act* de 1967, 18 USC 2510-2520, 1968);
- Ley para la protección en el alquiler de videos (*Video Privacy Protection Act*, 18 USC 2710, 1994);
- Ley de los registros telefónicos (*Telephone Consumer Privacy Act*, 47 USC 227, 1994);
- Ley del secreto bancario (*Bank Secrecy Act*, 31 USC 5313, 1994);
- Ley de archivos de los conductores (*Drivers Privacy Protection Act*, 18 USC 2721-25 1994);
- Ley sobre privacidad de los niños en sus actividades en Internet (Children's Online Privacy Protection Act, 15 USCA 6501-6506, 1998).

También existe legislación a nivel estatal, en este sentido la característica específica de la regulación en EUA es el carácter fragmentado de la norma. A diferencia de la Unión Europea, que tiene leyes bastante estrictas y unificadas sobre la privacidad, los Estados Unidos tienen leyes de protección de datos sectoriales. Las leyes de protección de datos pretenden proteger la información personal de un individuo del uso discriminado y sin consentimiento. La información que puede ser objeto de protección en los Estados Unidos incluye a los registros de salud y la información del crédito (Wacks, 2010).

Una de las leyes de protección de datos más amplias en los Estados Unidos es la Ley de Transferibilidad y Responsabilidad del Seguro Sanitario (HIPAA, por sus siglas en inglés). Esta ley federal, promulgada en 1996, crea protecciones para información relacionada con la salud individual. Específicamente, HIPAA especifica quien puede tener acceso a su información de salud. Por lo general, dicha información sólo está disponible para los médicos que la están usando para fines de coordinación de atención y tratamiento. La información que está sujeta a protección incluye las notas de los proveedores de servicios médicos, los registros de la aseguradora de salud, las conversaciones entre médicos y los tratamientos indicados.

Otra Ley es la Federal de Transacciones Crediticias Justas y Exactas (FACTA, por sus siglas en inglés) aprobada en 2003, diseñada para ayudar a proteger la información crediticia de los consumidores con respecto a los riesgos asociados con el robo de datos. Específicamente FACTA hace ilegal que los recibos de tarjetas de crédito y débito listen más de los últimos cinco

dígitos del número de la tarjeta, aunque esto no se aplica en los recibos escritos a mano. Además, FACTA limita la publicidad del número de seguridad social, al realizar una petición del informe crediticio.

La Ley de Protección de la Privacidad de Menores de los Estados Unidos (COPPA, por sus siglas en inglés) fue aprobada en 1998 como un medio para proteger la privacidad de los niños de menos de 13 años. Regula los sitios web que están dirigidos a niños o que se tiene conocimiento de su posible visita o uso. Dicha ley requiere que estos sitios web publiquen las políticas de privacidad en el sitio y adviertan si la información personal está siendo recopilada, cómo está siendo utilizada y cuáles son las prácticas de divulgación del operador del sitio. Estos sitios también deben obtener el consentimiento paterno verificable para recopilar la información de los niños. El proveedor debe, a petición de los padres, proporcionar una descripción del tipo de información que se colecta y cesar la recolección futura de datos del niño en particular.

Estas son sólo algunas de las leyes sectoriales sobre la privacidad de la información de personas en los EUA, lo cual muestra la diversidad de normas aplicadas y lo complejo que suele ser el control de los datos por parte de las personas. Aquí se parte de la premisa de que es la empresa quien trata los datos y la persona quien puede limitar el uso o tratamiento. A partir de estos criterios encontrados en el modelo sectorial de los EUA, podemos identificar en las siguientes líneas el diseño institucional y el organizacional creado para la protección de los datos personales por medio del derecho a la privacidad.

2.2.4 Diseño institucional

La historia de este modelo no surge, como la mayoría piensa, a partir del ensayo sobre la privacidad de Warren y Brandeis. Surge primero como un derecho superior a la libertad, no sólo de la persona, sino del pueblo de los EUA. Este derecho se transfiere como inalienable a la persona en lo particular para brindarle, asegurarle y reconocerle un espacio de libertad fuera del alcance del poder del Estado, de sus reglas y sus limitaciones. En principio fue la no interferencia del Estado, luego fue el respeto a la intimidad y sólo así fue que surge el derecho a *ser dejado solo*, pues con estos antecedentes como argumentos fue que se logró constituir lo que Warren y Brandeis en 1890 definieron como *el derecho a la privacidad* (E. Igo, 2018)

Estos dos abogados de Harvard sentaron las bases de la protección de la privacidad. En un artículo llamado *The Right to Privacy* (El derecho a la privacidad) Samuel D. Warren and Louis D. Brandeis se hacen eco del vertiginoso desarrollo de la prensa (apoyado por los rápidos avances

tecnológicos de entonces, sobre todo en cuanto a la fotografía y la proliferación de las primeras cámaras portátiles) y de las incipientes formas de vulneración del derecho a la intimidad personal.

Este artículo, que tuvo gran influencia en el Derecho de EUA (tengamos en cuenta que el Derecho anglosajón sienta sus bases sobre las sentencias dictadas por los tribunales de justicia) y continúa siendo un punto de referencia jurídico. Uno de los principales postulados del escrito describe el pilar básico de la legislación sobre protección de datos: el principio del consentimiento. En el artículo e*l derecho a la privacidad* se lee: "el derecho a la intimidad cede ante el consentimiento del individuo". Este derecho, según Dorothy J. Glancy (1979) en el Derecho consuetudinario ya existía y "encarnaba protecciones para la inviolabilidad de la personalidad de cada individuo". En este sentido el derecho a la privacidad desde el punto de vista consuetudinario asegura a "cada individuo el derecho a determinar en qué medida sus pensamientos, sentimientos y emociones se comunicarán a otros. Asimismo, fija los límites de la publicidad que cada individuo indica. En este sentido, para sus inventores, el derecho a la privacidad significa que cada individuo tenía derecho a optar por compartir o no compartir con los demás la información acerca de su "vida privada, los hábitos, los actos, y sus relaciones personales."

Warren y Brandeis (1890) argumentaron que era necesario para el sistema legal reconocer el derecho a la privacidad, ya que cuando la información sobre la vida privada de una persona se pone a disposición de los demás puede influir en la lesión a "la esencia misma de su personalidad y estimación". El concepto original del derecho a la intimidad se refiere a una penetración psicológica de la personalidad, donde la propia imagen puede verse afectada y a veces distorsionada o lesionada cuando la información de la vida privada queda a disposición de otras personas. "En términos más simples, para Warren y Brandeis el derecho a la privacidad es el derecho de cada individuo a proteger su integridad psicológica mediante el ejercicio del control de la información que puede reflejar y afectar su personalidad" (Glancy, 1979: 2). Esto es similar a lo que identificamos en términos de cómo se vuelve la protección de datos un derecho. Se constituye como tal a partir de sus antecedentes: el derecho a la intimidad, el de la privacidad y solo ante la complejidad del contexto tecnológico y comercial, se define como el derecho a la protección de datos personales.

Entonces el derecho a la intimidad no era nuevo cuando Warren y Brandeis escribieron su artículo en 1890. La frase "el derecho a ser dejado sólo", incluso fue una alusión al trabajo sobre *The Treatise on the Law of Torts* de Thomas Cooley en 1879. La definición del derecho a la privacidad en realidad proviene de una variedad de conceptos legales que tienen como precedente

diversas áreas de leyes comunes, tales como las leyes de contratos, de bienes, fideicomisos, derechos de autor, protección de secretos comerciales y agravios. De estas leyes desprendieron los principios que subyacen en todas ellas. El principio que subyace es la libertad.

El derecho a la privacidad, según la sistematización jurídica de los Estados Unidos y posterior a la Guerra Civil es colocado como el "derecho a ser dejado solo", el cual era en sí mismo parte de un derecho más general, el derecho a disfrutar la vida, que a su vez parte del derecho fundamental del individuo a la vida, y el derecho a la vida era parte de la tríada inherente de los derechos fundamentales reconocidos en la Quinta Enmienda de la Constitución de los Estados Unidos: "… ni sele privará de la vida, la libertad o la propiedad sin el debido proceso legal". De allí que la libertad sea un derecho inherente a la vida, a la libertad y a la propiedad. Este diseño constitucional está fundado en principios inherentes a la formación del Estado liberal de los Estados Unidos (E. Igor, 2018)

La privacidad como derecho se encuentra inserto en otros derechos como un principio inherente a otros de mayor trascendencia. Es un derecho intermediario que permite disfrutar de la vida, de la libertad y de la propiedad. Es instrumental en la medida que al protegerlo se protegen principios superiores. Este es el modelo que originó este sistema sectorial de protección, con amplio arraigo en EUA. Un modelo de protección de datos, que más bien se concibe como un modelo de protección de la privacidad.

2.2.5 Diseño organizacional

Por su origen normativo, la privacidad en Estados Unidos se protege principalmente en tribunales que bien pueden ser administrativos, civiles, penales, mercantiles por medio de un litigio entre particulares. En el caso del sector público existen autoridades administrativas sectoriales, como el caso del Departamento de Comercio (*Department of Commerce*), de Justicia (*Department of Justice*) y su oficina sobre la privacidad y las libertades civiles o el Departamento de Seguridad Nacional (*Homeland Security*), por mencionar algunos. Cada autoridad gubernamental se encarga de planear y ejecutar acciones específicas, según sus competencias (Weinstein, 2013).

A los tribunales les compete decir, interpretar el derecho según los principios constitucionales fundamentales o según leyes federales de materias específicas; a las autoridades gubernamentales aplicar las leyes generales y específicas en materia de privacidad. Entre las leyes federales están: la Ley de privacidad de 1974, la Ley de gobierno electrónico de 2002, así como las leyes específicas para el comercio.

En años recientes, aunque los EUA no tienen ninguna autoridad nacional de protección de datos personales, la Comisión Federal de Comercio (CFC) ha presentado fuertes disputas contra empresas tanto nacionales como internacionales, y se está constituyendo en la práctica como una Autoridad de Protección de Datos de Estados Unidos sustentando sus facultades en la sección 5 de la Ley de la Comisión Federal de Comercio, que prohíbe las prácticas comerciales injustas o engañosas. La CFC ha acusado a las empresas víctimas de las violaciones de datos con las prácticas comerciales desleales o engañosas sobre la base de que las infracciones fueron el resultado del fracaso de las empresas en adoptar medidas de seguridad razonables. La defensa se presenta ante tribunales y se diputa un litigio contra empresas que no cumplen las normas de seguridad razonables. Este modelo atiende a las resoluciones de los juicios entre particulares, regularmente empresas contra el sector gobierno representados por la comisión (FTC, 2000).

La CFC ha realizado diversas acciones sobre privacidad y seguridad de datos. En los últimos años ha interpuesto demandas por violación a la privacidad, infracciones, investigaciones sobre cambios de política de privacidad, incluso las anunciadas recientemente por Facebook y la privacidad en sistemas de análisis de grandes datos (*Big Data*). Como se puede observar, la Comisión Federal de Comercio se está constituyendo como la autoridad federal de protección de los datos personales y la privacidad, pero sólo en relación con los datos tratados por el sector privado (FTC, 2000). El sistema de administración está tratando de preservar la relación entre el sistema de protección de la Unión Europea y el de los Estados Unidos, así como la percepción endeble que se tiene sobre la debilidad en la aplicación del respeto a la privacidad, y es por medio de la Comisión Federal de Comercio que se está dirigiendo este diseño organizacional con la autoridad en los Estados Unidos.

Al final el tipo de organización de las autoridades garantes en materia de protección de datos personales va acorde con el sistema institucional-legal de protección. Es decir, un sistema normativo sectorial origina un sistema organizativo de autoridad descentralizado y disperso, donde por medio de los tribunales se brindan las únicas opciones de protección del individuo.

2.3 Interacción de ambos modelos para la protección internacional

En Europa la diferencia entre privacidad y datos personales suele entenderse. Existen sistemas como el español que lo definen claramente como protección de datos personales, otros como el alemán que lo denominan autodeterminación informativa y otros más, como en el caso de Inglaterra, que lo definen como privacidad.

Uno de los momentos más importantes de la privacidad y la protección de datos en Europa fue la redacción de la Directiva 95/46/CE. Ahora recientemente (2016) se aprobó el nuevo Reglamento Europeo de Protección de Datos Personales que dejará fuera la directiva 95 de la CE. Esto traerá consigo cambios que será necesario considerar. En esta investigación se trata en el caso de estudio algo sobre este reglamento, pero en realidad es un tema que se dejará como propuesta en el apartado de conclusiones de esta investigación.

Continuando con la manera en cómo se relacionan ambos modelos se tiene que en EUA se creó un marco de privacidad denominado puerto seguro o *Safe Harbor*. Este marco de puerto seguro fue hecho con el fin de crear estándares internacionales de privacidad que fueran más o menos compatibles con el sistema de protección solicitado por la Comunidad Europea.

Es necesario aclarar que este marco no asegura o determina que Estados Unidos sea un país con amplios estándares de seguridad en términos de la privacidad o la protección de los datos personales, más bien dice que determinadas entidades o empresas de ese país cuando estén adheridas a los principios *Safe Harbor* tienen los estándares mínimos que permiten intercambios de información. Esto es en realidad un contrato de transferencia, uso y tratamiento internacional de datos personales. Por lo tanto, no es más que la aplicación de los principios más importantes de seguridad de datos del modelo europeo en determinadas entidades (normalmente empresas) de EUA, que voluntariamente se adhieren a sus postulados.

En abril de 2004 la Comisión Europea de Justicia elaboró un minucioso estudio sobre el estado de la aplicación del puerto seguro en Estados Unidos. Como resultado, se encontraron importantes deficiencias que ocasionaban que los principios de puerto seguro quedaran en aplicación débil sobre los principios de privacidad y protección de datos –según el modelo garantista–, en una ilusión optimista que distaba mucho de la realidad. Las graves deficiencias encontradas fueron las siguientes (Galván, 2010):

- En cuanto al deber de información, se encontraron importantes dificultades por la falta de transparencia y por la inteligibilidad de la información proporcionada. Las políticas de privacidad eran farragosas y de difícil comprensión, y con demasiada frecuencia no proporcionaban una visión sobre las actividades a las que se refería el tratamiento de datos.
- No se hacía referencia al principio básico del consentimiento, entendiendo la Comisión Europea que este es un derecho crucial, a tener un control mínimo sobre el tratamiento de los datos personales, de los afectados o interesados.

- Respecto a las transferencias a terceros, el concepto de "tercero" no siempre quedaba definido (socio, filial, miembro de grupo de empresas, etc.) estando ausente en muchos casos el compromiso de ese tercero de cumplir con las prescripciones de *Safe Harbor*. El estudio hace una muy importante reflexión sobre la aplicación de este principio: "la flexibilidad que ofrece este principio se podría utilizar para eludir la legislación de la UE".
- El principio del acceso tendía a estar muy difuminado en la práctica, ofreciendo las empresas simplemente una información o dirección de contacto, sin precisar qué posibilidades o derechos se nos permitía ejercitar a través de esas direcciones. Otras veces, ni siquiera esa información de contacto estaba presente.
- La integridad o calidad de los datos tampoco se hacía efectiva correctamente, siendo difícil determinar la adecuación o pertinencia de los datos en relación con las actividades o finalidades previstas.

Otros estudios sobre *Safe Harbor* han dado como resultado un escandaloso descontrol en cuanto a las empresas adheridas a este marco: listado desfasado de empresas (donde aparecen entidades que ya no existen o que han quedado fuera de *Safe Harbor*), empresas incluidas en la relación de entidades adheridas pero que carecen de política de privacidad; también se encontró que la mayoría de empresas adheridas no cumplía con el séptimo principio (o lo hacían impracticable) relativo al mecanismo de resolución de controversias.

La Directiva de la Comisión Europea sobre protección de datos entró en vigor en octubre de 1998, y prohíbe la transferencia de datos de carácter personal a países no pertenecientes a la Unión Europea que no cumplen con la adecuación estándar de protección de datos dentro de ésta. En este sentido, cualquier entidad estadounidense que quisiera ser receptora de transferencias internacionales de datos de carácter personal procedentes de la Unión Europea tiene que adherirse al acuerdo *Safe Harbor*. Por lo que, si una organización está adherida a dicho acuerdo, se considera que cumple con los principios de privacidad necesarios, y el destino es confiable o cumple con los estándares necesarios de seguridad y privacidad.

Una de las graves deficiencias de dicho acuerdo es que la verificación del cumplimiento la realizan las propias entidades sin un control externo; en España estas competencias son asumidas por la Agencia Española de Protección de Datos. Esto, unido a la libre interpretación de los principios, hace que el nivel de protección o acceso aplicado a la información pueda ser insuficiente. Además, otros estudios sobre *Safe Harbor* han dado como resultado un descontrol en

cuanto a las empresas adheridas a este marco: listado desfasado de empresas (donde aparecen entidades que ya no existen o que han quedado fuera del modelo de transferencias internacionales). Analicemos con un poco más este marco de privacidad.

2.3.1 Safe Harbord

Safe Harbor, o puerto seguro, establece los principios de privacidad estandarizados con la normativa europea mediante una certificación. Una vez obtenida la certificación, permite transferencias dentro del Espacio Económico Europeo (EEE), el cual incluye a Suiza y los Estados Unidos. El objetivo fue permitir a las empresas de EUA cumplir con un requisito indispensable para realizar actividades económicas, sociales o políticas que implicaran el tratamiento de datos personales y tuvieran necesariamente relación con la Comunidad Europea. En este sentido, cuando se logran estandarizar se reconoce que Estados Unidos cuenta con una protección adecuada según los principios europeos; esta certificación también la pueden obtener empresas o corporativos, e incluso las leyes nacionales; se denomina nivel de adecuado de protección de datos personales. Es un estándar internacional que la Comunidad Europea impuso para proteger el manejo de la información personal en posesión de un tercero.

El sistema de protección de datos personales de la Unión Europea establece un sistema altamente proteccionista (Kobrin, 2004: 118), por ello no se permite realizar transferencias de datos personales a quienes no cuentan con este sistema de estandarización de la norma. La negociación entre Estados Unidos y la Unión Europea la iniciaron David Aron, a cargo de la Secretaría de Comercio, y John Mogg director general de Mercado interno (Kobrin 2004: 120). El Departamento de Comercio lo propuso en 1998 y fue aceptado hasta el año 2000 por la Comisión Europea.

Para obtener el calificativo de S*afe Harbor* se deben cumplir los siguientes principios descritos en la Directiva 95/46/CE:

1) Información. Los interesados deberán ser informados de que sus datos personales están siendo recogidos y que serán tratados únicamente con la finalidad para la que fueron recogidos.
2) Elección. Los interesados tendrán el derecho de cancelación y oposición a que sus datos sean recogidos una vez sean recabados y a oponerse a la cesión o transferencia a terceros.

3) Transferencia progresiva. La cesión de datos a terceros se llevará a cabo con organizaciones que también garanticen un adecuado nivel de cumplimiento de protección de datos.
4) Seguridad. Se deben establecer y cumplir determinadas medidas de seguridad para prevenir pérdidas de información y accesos no autorizados.
5) Integridad de los datos. Los datos deberán ser relevantes y exactos para el propósito para el que fueron recogidos.
6) Acceso. Los interesados podrán acceder en todo momento a la información que haya sido recabada acerca de ellos y podrán corregirla o eliminarla si es inexacta o inadecuada.
7) Ejecución. Se deben destinar medios y recursos para garantizar el debido cumplimiento de estos principios" (Murphy, 2001: 158).

Una vez obtenido el certificado, éste se debe renovar anualmente. Pueden hacerlo de forma interna (para verificar que se cumplan dichos principios) o de forma externa (auditorías). Hay también seguimiento para que se proporcione a los empleados la formación adecuada en esta materia y también se reconocen mecanismos de solución de conflictos. Esta es la manera general sobre cómo funciona la relación entre ambos modelos. Sin embargo, estas normas han cambiado por el marco para proteger la privacidad (*Privacy Shield Framework*), el cual analizaremos en el siguiente apartado.

2.3.2 Privacy Shield Framework

Como consecuencia de la problemática que se presentaba con el marco *Safe Harbord*, el 6 de octubre de 2015 el Tribunal de Justicia de la Comunidad Europea emitió una sentencia declarando inválida la Decisión 2000/520/CE de la Comisión Europea, del 26 de julio del año 2000, sobre la adecuación de la protección proporcionada por los principios de privacidad, según el Departamento de Comercio de los Estados Unidos. De acuerdo con esa decisión, este marco ya no sería válido como un mecanismo para cumplir los requisitos de la Unión Europea en materia de protección de datos al transferir datos personales de la Unión Europea a los Estados Unidos.

Esta decisión originó que se rediseñara el marco de protección de la privacidad estandarizado de los Estados Unidos para el intercambio de datos con la UE, por lo que el 12 de julio de 2016 la Secretaria de Comercio estadounidense Penny Pritzker se unió a la Comisaria de

la Unión Europea, Věra Jourová, para anunciar la aprobación de la Unión Europea y los Estados Unidos el uso de *Privacy Shield Framework*, que reemplazaría al *Safe Harbor* de Estados Unidos. A partir del 1 de agosto de 2016 se iniciaron las certificaciones con base en este nuevo marco de cooperación y adecuación (US *Department of Commerce*, 2016).

El objetivo, tal como se menciona, es ofrecer un mecanismo de protección a las personas cuando se trasfieren datos personales de la Unión Europea a los Estados Unidos. En virtud de fomentar y promover el desarrollo del comercio internacional y el desarrollo de la industria. Dentro de los principios que se contemplan están el de información y notificación; elección, *accountability*; seguridad, integridad del dato, limitación de propósito de uso de datos y el acceso, entre otros. Estos principios se refuerzan con algunos complementos como la protección especial de los datos sensibles, excepciones sobre la información sobre periodistas, así como un sistema de cooperación con autoridades de la protección de datos personales para realizar investigaciones (US *Department of Commerce*, 2016) o las funciones necesarias para lograr una adecuada protección de la información personal.

Estos principios pueden ser limitados por la seguridad nacional, el interés público o por la aplicación de la ley, estatutos, regulación o jurisprudencia que origine conflictos con el seguimiento de los mismos principios de protección. Como se puede observar, estos son los dos grandes modelos de protección de datos personales con implicaciones económicas y políticas.

Por un lado, tenemos el modelo de la Unión Europea con mayores garantías ante las implicaciones o afectaciones a la sociedad por un contexto digital, el cual no deja de reconocer el valor económico de esta información. Por otro, el diseño de los EUA reconocido como sectorial, con mecanismos de regulación, desregulación y autorregulación principalmente económica para el sector privado, con una influencia económica mayor para México que la UE. Estos son los modelos que influyeron en el diseño institucional y organizacional para la protección de datos personales en México, modelos con los cuales tiene amplias relaciones comerciales y políticas. De allí la influencia e importancia de haberlos analizado, pues permite ir integrando las características que se retomaron de cada modelo para el diseño del modelo mexicano.

CAPÍTULO 3. EL DISEÑO INSTITUCIONAL Y ORGANIZACIONAL EN MÉXICO

"Dicen que hay dos cosas que no conviene saber cómo se hacen:
las salchichas y las leyes"
Alfredo Reyes Krafft

En este capítulo se analiza la manera en cómo se diseñó el modelo de protección de datos personales en México. Iniciamos con el análisis histórico de las primeras propuestas de ley en 2001 y se concluye en lo general con la ley general aprobada en 2016. Este análisis incluye explicar los objetivos, los intereses, los actores y el contexto que son los marcos institucionales en torno a la protección de los datos personales; los valores que animan la vida de las acciones; los comportamientos personales y colectivos; las normas y procedimientos que dan certidumbre y hacen posible el desempeño regular y ordenado de las actividades sociales vinculadas al ejercicio, garantía y control de este derecho humano fundamental, la protección de datos personales.

Para cumplir el objetivo el contenido se estructura en dos grandes apartados: el primero corresponde al diseño institucional y el segundo al diseño organizacional de la autoridad garante. En el primero se identifican algunos momentos históricos clave sobre el proceso de regulación de la protección de datos, donde se definieron las normas, los códigos de conducta, los valores y los intereses en torno a los datos personales en México. En el segundo apartado se identifican los modelos de autoridades que definen la estructura organizacional gubernamental para el control y garantía de este derecho.

3.1 Diseño institucional

En México la regulación que existe sobre protección de datos personales está dividida en regulación aplicada al sector público y la aplicada al sector privado. Antes de 2001 no se había presentado alguna iniciativa de ley o regulación específica sobre el tema. Existía en la norma como parte de otras leyes e integrada a la privacidad y a la intimidad. Estas normas aún se encuentran vigentes, por ejemplo: la Ley de Protección al Consumidor de 1992 en sus artículos 16 a 18 bis y 76 bis, así como en el artículo 103 bis de la Ley General de Salud (Recio, 2014: 1). Otras leyes también aplicables son, la Ley de Instituciones de Crédito; la Ley para regular las Sociedades de Información Crediticia; la Ley Federal del Derecho de Autor que en su articulado prevé la

protección jurídica a las bases de datos; así como el Código Civil y el Código de Comercio en lo relativo al Registro Público (Alfredo Reyes Krafft, entrevista personal, 4 de diciembre de 2014). De la misma manera, y dado que un daño a la persona debe tener diferentes medios de defensa, también el derecho penal posee herramientas de protección efectivas que se incorporan al conjunto de protección de las personas en su integridad e identidad, de allí que la privacidad como derecho también esté prevista como un medio de defensa (Román Sánchez, 2014).

Entonces, antes de la primera iniciativa se debe contemplar que, si bien la protección de datos personales no estaba prevista de manera específica en las leyes mexicanas, la realidad es que el derecho a la privacidad y a la intimidad sí estaban integradas en normas civiles, de protección al consumidor, financieras, mercantiles y en las penales. En este sentido la protección de datos (PD) es un derecho nuevo, "lo que no es nuevo ni de reciente creación es la protección constitucional en México para la protección de la vida privada de las personas y en ese sentido se tiene amplia doctrina jurisdiccional en la materia […], mediante la interpretación de los artículos 6º, 7º y 16° constitucionales, donde se establecieron cuáles iban a ser las razones por las cuales el Estado podía interferir en la vida privada de las personas. Esta protección es considerada en el estudio del derecho, como derechos de la personalidad que tienen una implicación en el honor, en los derechos de la reputación y que pueden tener un daño moral establecido y justificado en un momento específico. Para estos casos existe una jurisprudencia ya establecida" (Issa Luna, entrevista personal, 18 de noviembre de 2014)

Lo nuevo, entonces, es la protección de datos personales como un derecho humano fundamental que se manifiesta en la Constitución hasta el año 2011 como un derecho individual y en este sentido "no existe todavía, a la fecha, una jurisprudencia amplia ni sustancial sobre el derecho a la protección de datos personales, lo cual no permitía conocer sus alcances y límites" (Issa Luna, entrevista personal, 18 de noviembre de 2014).

En México la regulación en materia de protección de datos personales tiene tres etapas: primero se reguló de manera muy general en el ámbito público, posteriormente en el privado y finalmente se crearon normas generales en la materia. En el siguiente apartado analizaremos las dos primeras etapas, por ser el objetivo de esta investigación.

3.1.1 Regulación en el sector público

El 11 de junio del 2002 se publicó en el Diario Oficial de la Federación la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG). Esta ley contiene en

dos capítulos referentes a la protección de datos personales: el capítulo 3 y el 4. El tercero versa sobre la información reservada y la confidencial; los datos personales se encuentran incluidos en la información confidencial (artículo 18 de la LFTAIPG). En el capítulo cuarto los datos personales son tratados desde el artículo 20 al 26. A partir de la legislación de trasparencia, la protección de datos entra en el escenario administrativo sólo como un límite del acceso a la información, pero también se constituye como una facultad más del IFAI en el ámbito público de su competencia.

El grupo Oaxaca[18] al promover el acceso a la información y el principio de máxima publicidad, no tuvo como "estrategia el tema de la protección de datos personales, la única forma en la cual quedaron protegidos los datos personales como parte del trabajo del grupo Oaxaca fueron los capítulos que otorgaban una mínima consideración, pues al no existir una legislación especializada en esa materia, sólo se incluyó para establecer un candado y un resguardo específico en la clasificación de la información" (Issa Luna, entrevista personal, 18 de noviembre de 2014), por lo que los datos personales no fue un tema prioritario dentro de los objetivos del grupo Oaxaca que promovió el derecho de acceso a la información pública en México.

Entonces la protección de datos personales en el sector público apareció formalmente como un límite del derecho de acceso a la información, específicamente en el capítulo 4, de la siguiente manera:

Cuadro 3. Artículos sobre protección de datos personales en la LFTAIPG

Artículo	Tema sobre datos personales
Art. 20	Responsabilidades de los sujetos obligados.
Art. 21	Limitación de sujetos obligados ante el tratamiento de datos personales
Art. 22	Ausencia de consentimiento en el tratamiento de datos en casos previstos por la ley
Art. 23	Sistema de datos personales y su conocimiento a la autoridad.
Art. 24	Solicitud de acceso a datos ante las autoridades competentes.
Art. 25	Rectificación de datos personales.
Art. 26	Negativa de solicitudes y recursos

Fuente: Elaboración propia, con datos del Capítulo 4 de la LFTAIPG.

Estos artículos otorgan sólo el derecho de acceso y corrección de los datos a los personas; limitan su uso, a menos que el tratamiento sea adecuado, pertinente y no excesivo en relación con los propósitos para los cuales se hayan obtenido; obligan a los sujetos que tratan datos personales a "poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales,

[18] Para profundizar en el tema consultar: Luna Pla, Issa. 2013 [2009]. *Movimiento social del derecho de acceso a la información en México*. Instituto de Investigaciones Jurídicas, UNAM. 1ª reimpresión.

el documento en el que se establezcan los propósitos para su tratamiento", es decir: informar sobre los objetivos del tratamiento y procurar que los datos personales sean exactos y actualizados. Asimismo, dice que los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar de los individuos a que haga referencia la información. Es importante mencionar que el artículo 22 hacía referencia a que la información por razones estadísticas, científicas o de interés general previstas en ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran, no requería consentimiento de los individuos. Este artículo posteriormente, en 2005, fue derogado.

El artículo 22 también consideraba la ausencia de consentimiento cuando se transmita entre sujetos obligados o entre dependencias y entidades, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos; cuando exista una orden judicial; a terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquellos para los cuales se les hubieren transmitido, así como en otros casos previstos por las leyes. Este artículo es importante en la medida que deja a las autoridades gubernamentales la disponibilidad de la información para el cumplimiento de sus funciones.

El sistema persona fue una herramienta que obligó a las autoridades del gobierno federal a dar a conocer los datos personales que tenían en su posesión, motivando su atribución en el artículo 23 y 61 de la ley. Con estos artículos, el tratamiento de los datos personales en el sector público aparece en la agenda pública como un límite a otro derecho: el acceso a la información. Este límite se basa en el fundamento que tiene el Estado de tener control sobre la información de las personas cuando les proporciona servicios, derechos y les exige obligaciones.

María Marván dice que "cuando se propone la ley de transparencia se preguntaban sobre los límites del acceso a documentos del gobierno, pues evidentemente todo derecho tiene límites. En la propuesta se establecieron dos: los documentos que son reservados de manera temporal, con justificación legal que afecte la seguridad nacional, y los documentos que sean o contengan datos personales de los gobernados fundamentalmente, más que de los funcionarios, porque los gobiernos para poder gobernar manejan grandes cantidades de documentos que tienen datos personales. Un ejemplo son los expedientes clínicos del Seguro Social, que sólo el titular puede solicitar. Entonces, ahí aparece clarísima la necesidad jurídica de poner los datos personales como una

limitante al derecho de acceso a la información pública, y como ese caso hay otros tipos de documentos que manejan los gobiernos" (María Marván, entrevista personal, 29 de octubre de 2014).

Por lo tanto, se reconoce que el gobierno maneja grandes cantidades de información necesaria para dar servicios, otorgar derechos y exigir obligaciones. Datos que están a su resguardo y que implica el control de su uso, conocer la información básica sobre cada una de las personas que se encuentra en territorio nacional (nacionales o no), incluso de aquellas personas nacionales que por diversos motivos se encuentran fuera de este territorio. Toda esta información no está concentrada en un solo organismo, en México existe dispersión de la información poblacional recolectada. Dentro de las grandes bases de datos está el registro civil, el registro federal de electores, el registro de afiliados a la seguridad social del Instituto Mexicano del Seguro Social (IMSS) o del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE), por poner algunos ejemplos.

Después de la ley, y al reconocer que el gobierno manejaba grandes cantidades de datos y que éstos tenían que ser protegidos, se profundizaron algunas disposiciones sobre el control de la información pública en el sector público. De esta manera se crearon lineamientos sobre protección de datos para observancia del sector público[19], algunos procedimientos específicos para acceso y rectificación de datos personales en posesión del sector público, así como la creación de un sistema de datos personales que incorporó un índice sobre la información que posee el sector público en su posesión. Este sistema se denominó "sistema persona", cuyo contenido muestra la información de las personas que poseen las autoridades. Estas disposiciones normativas secundarias, a partir de la LFTAIPG, fueron creadas por el IFAI como parte de sus facultades sobre protección de datos personales en posesión del sector público, fundamentados en el capítulo 4 de la Ley de Transparencia.

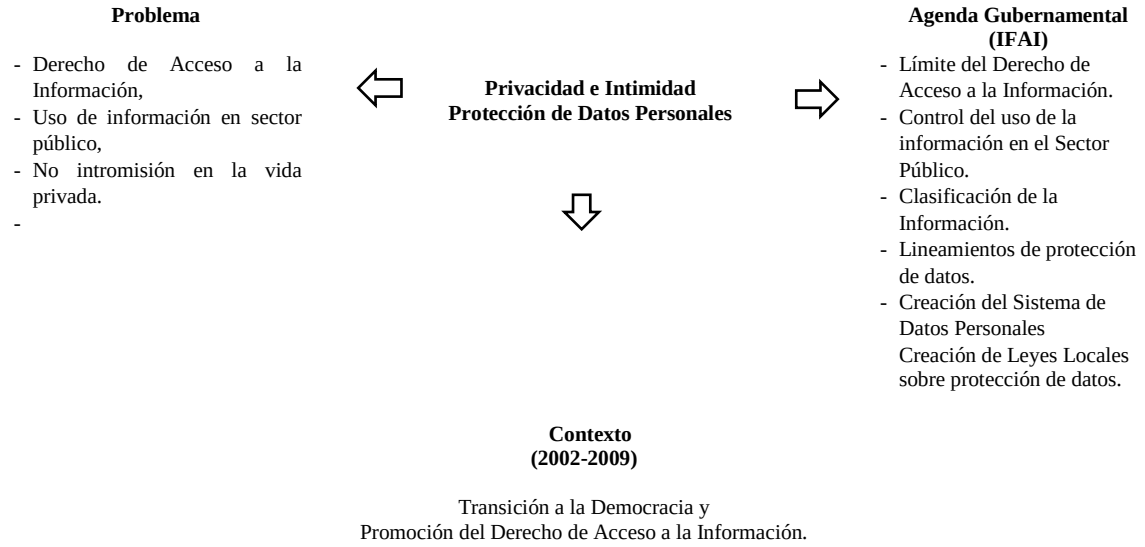
Esta regulación también incluyó algunas certificaciones específicas, por ejemplo: la norma de certificación del expediente electrónico que maneja el Instituto Mexicano del Seguro

[19] Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de corrección de datos personales que formulen los particulares; Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de acceso a datos personales que formulen los particulares, con exclusión de las solicitudes de corrección de datos personales; Lineamientos que deberán observar las dependencias y entidades de la administración pública Federal para notificar al Instituto el listado de sus sistemas de datos personales, y los lineamientos generales para la clasificación y desclasificación de la información de las dependencias de la Administración Pública Federal. IFAI, 2004. Primer Informe de Labores. México, Instituto Federal de Acceso a la Información, página 22.

Social y algunas dependencias del sistema de salud federal, y otras disposiciones sobre protección de datos en el sector público. Esquemáticamente el proceso de agenda y alternativas en torno a la protección de datos en el sector público fue el siguiente:

Esquema 10. Proceso de agenda para la protección de datos en el sector público

MODELO DE PROTECCIÓN DE DATOS EN EL SECTOR PÚBLICO.



Fuente: Elaboración propia.

Estas últimas acciones tuvieron como fundamento el artículo 33 de la LFTAIPG[20], así como los artículos 6[21] y 16[22] de la Constitución Política de los Estados Unidos Mexicanos (CPEUM). En este sentido fueron diseñados por el IFAI bajo la coordinación y la dirección, principalmente, de Lina Ornelas, Edgardo Martínez y su equipo integrado en el área de clasificación de la información. "Dentro de los asuntos de clasificación de información se presentan algunos casos donde se determina si puedes o no puedes tener acceso a datos personales, derivado de una solicitud de

[20] Artículo 33. El Instituto Federal de Acceso a la Información Pública es un órgano de la Administración Pública Federal, con autonomía operativa, presupuestaria y de decisión, encargado de promover y difundir el ejercicio del derecho de acceso a la información; resolver sobre la negativa a las solicitudes de acceso a la información y *proteger los datos personales en poder de las dependencias y entidades*. El subrayado y en negritas intencional.

[21] Artículo 6° constitucional, apartado A, fracción 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".

[22] Artículo 16 constitucional, párrafo segundo: "Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de estos, 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."

acceso a información pública, y justo allí está el vínculo entre acceso a la información y datos personales" (Edgardo Martínez, entrevista personal, 7 de noviembre del 2014).

Entonces la protección de datos surge en la legislación como un límite del acceso a la información; sin embargo, el propio Instituto fue promoviendo –como parte de su agenda interna– el ejercicio de la protección de datos personales en posesión del sector público. Primero fue la ley, luego el reglamento; los lineamientos de acceso y rectificación de datos personales en el sector público; el sistema de datos personales; los lineamientos de protección de datos personales; el certificado del expediente clínico electrónico y las dos evaluaciones de impacto a la privacidad: la del expediente clínico electrónico en el Servicio de Salud Federal, así como el de la cédula de identidad que manejó la Secretaría de Gobernación. Acciones que derivaron primero como límite del Acceso a la Información y posteriormente como parte de sus funciones, amparados en las facultades sobre protección de datos personales otorgadas al IFAI.

Las facultades del IFAI sobre protección de datos personales fueron otorgadas sólo para el tratamiento en el sector público, argumentando que no se contaba con las facultades constitucionales para legislar al respecto. Es importante recordar —aunque se estudia en el apartado posterior— que el 14 de febrero de 2001 se propuso una ley sobre protección de datos. El Senador Antonio García Torres, en la minuta que presentó en 2005 nuevamente para promover una legislación sobre protección de datos personales, dijo que en 2001 se le había dado prioridad a la Ley de Acceso a la Información, dejando de lado la de protección de datos personales que él había promovido desde 2001.

Se le dio prioridad al acceso a la información y fue una fusión de dos frentes: del Grupo Oaxaca y del ejecutivo federal: "la ley fue un consenso que se aprueba en 2002, se publica, y a partir de allí fue el referente para la creación de las leyes en las entidades federativas. También de ahí desencadenaron algunas leyes de protección de datos; no todos tienen leyes de protección de datos, para 2015 aproximadamente once entidades federativas poseían normas en la materia, sin embargo, tanto el tema de los datos personales, como el de archivos se quedó en mera advertencia, aunque por diferentes causas, razones jurídicas, quizás algunas políticas, no permitieron que viera la luz aquella iniciativa de ley de protección de datos, aunque sí la de transparencia" (entrevista a Edgardo Martínez, 7 de noviembre de 2014).

Una vez aprobada la ley de acceso a la información, para ponerla en práctica y promover su competencia sobre datos personales en posesión del sector público, el IFAI se apoyó de organizaciones internacionales afines al tema de protección de datos personales para motivar su

competencia y promover una ley federal de protección de datos personales. En noviembre del 2005 México fue sede del IV Encuentro Iberoamericano de Protección de Datos personales, celebrado en la ciudad de México y organizado por el IFAI, en colaboración con la Red Iberoamericana de Protección de Datos, la LV Legislatura del Estado de México y el Instituto de Transparencia y Acceso a la Información Pública de dicha entidad. Se contó con la participación de representantes de países como Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, el Salvador, España, Estados Unidos de América, Nicaragua, Perú, Reino Unido y Uruguay. Se discutieron temas como el derecho fundamental a la protección de los datos personales; las tecnologías de la información y su impacto en la privacidad de las personas; los desarrollos normativos y la globalización; la protección de los datos personales por los gobiernos, y la perspectiva del sector financiero y comercial en la protección de este tipo de datos. Al evento concurrieron funcionarios de las dependencias y entidades de la Administración Pública Federal; de los estados de Aguascalientes, Colima, Chihuahua, Estado de México, Querétaro, San Luis Potosí, Sinaloa y Zacatecas; medios de comunicación, así como representantes de organismos de la sociedad civil. Como resultado de este evento, el IFAI firmó dos cartas de intención de colaboración, una con la Agencia Española de Protección de Datos y la otra con la Dirección Nacional de Protección de Datos Personales de Argentina (IFAI, 2005: 23).

"Este fue un momento clave para el tema de protección de datos personales. A partir de allí se promovieron con mayor énfasis las propuestas de leyes específicas a nivel federal y a nivel local. Asimismo, existieron arduas negociaciones y pugnas porque el IFAI fuera la misma autoridad garante tanto del acceso a la información como de la protección de datos personales, pues existían propuestas que consideraban que debería crearse otra autoridad que se encargara de la protección de datos personales; otros consideraban que debería ser la Secretaría de Economía, otros la Procuraduría del Consumidor y así existieron diversas propuestas, pero el IFAI pugnó fuertemente por ser designado como el garante de este nuevo derecho en el ámbito privado, pues argumentó la capacidad técnica y experiencia en el ejercicio de este derecho en el sector público." (Jacobo Esquenazi, entrevista personal, 15 de diciembre del 2014).

La regulación en el sector público se complementó con la promulgación de leyes locales en las entidades federativas. México está dividido en 32 entidades federativas, incluyendo e1 Distrito Federal, ahora Ciudad de México. Sobre el tema se profundizará en el siguiente apartado.

3.1.1.1 Protección de datos personales en las entidades federativas

La aprobación de la LFTAIPG en 2002 “fue el gran referente para la creación de todos los estados de la república de leyes de acceso a información y luego también de ahí desencadenaron algunas leyes de protección de datos” (entrevista a Edgardo Martínez, 7 de noviembre del 2014).

En 2015, de las 32 entidades federativas 11 expidieron su propia ley de protección de datos personales: Campeche, Chihuahua, Colima, Distrito Federal, Durango, Estado de México, Guanajuato, Puebla, Oaxaca, Tlaxcala y Veracruz. El resto de las entidades tienen un apartado especial en la Ley de Transparencia y Acceso a la Información Pública. Los sujetos obligados que prevén las legislaciones locales se muestran en el siguiente cuadro.

Cuadro. 4. Sujetos obligados a las leyes locales de protección de datos personales.

N°	Entidad federativa	Ejecutivo	Legislativo	Judicial	Autónomos	Municipio	Partidos Políticos	Otros
1	Aguascalientes	Si	Si	Si	Si	Si	Si	Si
2	Baja California	Si	Si	Si	Si	Si	Si	Si
3	Baja California Sur	Si	Si	Si	Si	Si	No	Si
4	Campeche	Si	Si	Si	Si	Si	Si	Si
5	Chiapas	Si	Si	Si	Si	Si	No	No
6	Chihuahua	Si	Si	Si	Si	Si	Si	Si
7	Coahuila	Si	Si	Si	Si	Si	Si	Si
8	Colima	Si	Si	Si	Si	Si	S/D	Si
9	Distrito Federal	Si	Si	Si	Si	Si	Si	Si
10	Durango	Si	Si	Si	Si	Si	Si	Si
11	Estado de México	Si	Si	Si	Si	Si	No	Si
12	Guanajuato	Si	Si	Si	Si	Si	No	Si
13	Guerrero	Si	Si	Si	Si	Si	Si	Si
14	Hidalgo	Si	Si	Si	Si	Si	Si	Si
15	Jalisco	Si	Si	Si	Si	Si	Si	Si
16	Michoacán	Si	Si	Si	Si	Si	Si	Si
17	Morelos	Si	Si	Si	Si	Si	Si	Si
18	Nayarit	Si	Si	Si	Si	Si	Si	Si
19	Nuevo León	Si	Si	Si	Si	Si	No	Si
20	Oaxaca	Si	Si	Si	Si	Si	No	Si
21	Puebla	Si	Si	Si	Si	Si	Si	Si
22	Querétaro	Si	Si	Si	Si	Si	No	Si
23	Quintana Roo	Si	Si	Si	Si	Si	No	No
24	San Luís Potosí	Si	Si	Si	Si	Si	Si	Si
25	Sinaloa	Si	Si	Si	Si	Si	Si	Si
26	Sonora	Si	Si	Si	Si	Si	Si	Si
27	Tabasco	Si	Si	Si	Si	Si	Si	Si
28	Tamaulipas	Si	Si	Si	Si	Si	No	Si
29	Tlaxcala	Si	Si	Si	Si	Si	Si	Si
30	Veracruz	Si	Si	Si	Si	Si	Si	Si
31	Yucatán	Si	Si	Si	Si	Si	No	Si
32	Zacatecas	Si	Si	Si	Si	Si	Si	Si

Fuente: Guerra Ford, Oscar G. 29 de enero de 2014. *La protección de los datos personales en posesión del sector público y privado.* InfoDF, página 6.

De 11 entidades federativas que tienen leyes específicas sobre protección de datos personales y de

las 21 restantes, sólo Querétaro no garantizaba ningún derecho de Acceso, Rectificación, Cancelación y Oposición (ARCO), y Puebla sólo garantizaba el derecho de Rectificación, y todos los demás reconocían el derecho de Acceso y Rectificación. Las entidades que no garantizaban tanto el derecho de Cancelación y de Oposición son: Aguascalientes, Baja California Sur, Nayarit y Quintana Roo. Las entidades que no garantizan sólo Oposición son: Chiapas, Colima, Guanajuato, Hidalgo, Morelos, Sinaloa y Tabasco. (Guerra, 2014). Estas disparidades normativas, van a ser el motivo por el cual se tenga la necesidad de diseñar una ley general en materia de protección de datos personales, justo para tratar de equilibrar el ejercicio de derechos en territorio mexicano.

De las autoridades garantes en las entidades federativas en su mayoría no pertenece al Poder Ejecutivo, con excepción de Chiapas[23] y Zacatecas[24], las cuales no son organismos autónomos. Las demás entidades trabajaron en el diseño de sus autoridades con mayor autonomía. En 2002 se aprobaron cinco leyes locales de acceso a la información y transparencia: Jalisco, Sinaloa, Aguascalientes, Michoacán y Querétaro. Además de la ley Federal. En 2003 se aprobaron las leyes de Nuevo León, Colima, San Luis Potosí, Distrito Federal, Guanajuato, Morelos y Coahuila; en 2004 en el Estado de México, Quintana Roo, Yucatán, Veracruz, Nayarit, Zacatecas, Tlaxcala, Puebla y Tamaulipas; en 2005 Sonora, Baja California Sur, Campeche, Baja California, Guerrero y Chihuahua; en 2006 Oaxaca, Chiapas e Hidalgo. Finalmente, Tabasco aprobó su ley en 2007.

Entonces la promulgación de leyes de acceso a la información y transparencia inició en el año 2002, junto con la ley federal. Las primeras entidades federativas en contar con una ley de transparencia fueron Jalisco y Sinaloa. Los estados de Oaxaca, Chiapas, Hidalgo y Tabasco fueron los últimos en contar con una ley. A partir de allí la protección de datos personales quedó garantizada y protegida en ámbitos estales y municipales dentro del sector público, sólo para el

[23] Ley que Garantiza la Transparencia y el Derecho a la Información Pública para el Estado de Chiapas. 12 de octubre de 2006. Artículo 60.- El Instituto de Acceso a !a Información Pública de la Administración Pública Estatal, es un organismo público descentralizado no sectorizable de la referida administración pública estatal, con personalidad jurídica .y patrimonio propios, autonomía de gestión, así como facultades de operación, decisión, resolución, administración, fomento, promoción y sanción en lo concerniente al derecho de acceso a la información pública, a que se encuentran obligados los sujetos previstos en el artículo 2° de esta ley.

[24] "Ley de Transparencia y Acceso a la Información Pública del Estado de Zacatecas. Artículo 91. La comisión Estatal para el Acceso a la Información pública es un organismo público descentralizado de la administración pública estatal, con autonomía presupuestaria, operativa y de decisión." La primera ley fue promulgada el 14 de julio de 2004 y la última reforma corresponde al 2 de diciembre de 2010. Asimismo, ver anexo 1. Autonomía de los órganos garantes. Guerra Ford, Oscar. 29 de enero de 2014. *La protección de los datos personales en posesión del sector público y privado.* InfoDF. Página 6.

caso de la información pública y de una manera muy general, poco sistematizada y con alcance menor. Las leyes de protección de datos personales que se promulgaron en 11 de las entidades federativas lo hicieron en las siguientes fechas.

Cuadro 5. Expedición de leyes locales.

Ley de Protección de Datos en las Entidades Federativas con fecha de expedición.	
Campeche	19 de junio de 2012 21 de enero de 2013 (reformada)
Estado de México	13 de agosto de 2012
Tlaxcala	14 de mayo de 2012
Distrito Federal	03 de octubre de 2008 20 de agosto de 2014 (reformada) 28 de noviembre de 2014 (reformada)
Chihuahua	26 de junio de 2013
Colima	21 de junio de 2003
Durango	5 de diciembre de 2013 26 de diciembre de 2014 (reformada)
Guanajuato	19 de mayo de 2006
Oaxaca	23 de agosto de 2008
Puebla	25 de noviembre de 2013
Veracruz	15 de enero de 2010

Fuente. Elaboración propia con datos de las leyes locales hasta 2015.

La regulación en materia de protección de datos personales en las entidades federativas se puede dividir en tres: las que regulan la protección de datos con base en la ley de acceso a la información, las que fundan su protección tanto en la ley de acceso a la información y en la de protección de datos, y los que tienen una ley específica sobre protección de datos. El esquema se muestra de la siguiente manera:

Cuadro 6. Tipología de la regulación en las entidades federales.

REGULACIÓN DE LA PROTECCIÓN DE DATOS EN LAS ENTIDADES FEDERATIVAS.	
Ley de Protección de Datos	Campeche, Colima, Distrito Federal, Guanajuato, Estado de México, Durango, Chihuahua, Guanajuato, Oaxaca, Puebla.
Ley de Acceso a la Información y Protección de Datos	Coahuila y Morelos.
Ley de Acceso a la Información de la entidad	Aguascalientes, Baja California, Baja California Sur, Campeche, Chiapas, Coahuila, Guerrero, Hidalgo, Jalisco, Michoacán, Nayarit, Nuevo León, Querétaro, Quintana Roo, San Luis Potosí, Sinaloa, Sonora, Tabasco y Tamaulipas.

Fuente. Elaboración propia. Información hasta el año 2015.

Para el diseño normativo y la decisión de las autoridades garantes de la protección de datos personales se consideró el contexto constitucional y administrativo del sistema federal mexicano. Esto se puede entender por tres principales características:

1. La normativa local que existía antes de la LFTAIPG y de la ley de protección de datos personales en posesión de los particulares. En México antes de 2001 algunas constituciones locales ya consideraban el sistema de protección como habeas corpus o habeas data.
2. El sistema de gobierno federal, con autonomía regulativa para las entidades federativas.
3. Las competencias del poder legislativo para poder legislar sobre protección de datos personales a nivel federal.

Esto originó un conjunto diferenciado de normas, procedimientos y estructuras organizacionales diversas, pero sobre todo dio lugar a la descentralización, la fragmentación tanto en procedimientos, funciones y estructuras de autoridad. Parafraseando a Casar y Maldonado (2010) este diseño institucional de las autoridades garantes fueron producto de los distintos marcos institucionales; constitucionales, por la existencia misma de ventanas de oportunidad, la maniobra constitucional de las entidades y del repertorio de estrategias disponibles en la esfera pública para organizar la respuesta del Estado por la vía de políticas públicas regulativas a la protección de datos personales en las entidades federativas.

En el siguiente apartado se analiza el diseño institucional y de las autoridades garantes en materia de protección de datos personales en el sector privado.

3.1.2 Regulación en el sector privado

Privacidad y protección de datos personales están vinculados, pero ambos principios y derechos son diferentes en su forma y contenido (ver capítulo 1). La privacidad como derecho vinculado a la libertad, al honor y a la propia imagen se encuentra en la legislación mexicana como parte de otras normas, como la civil, la penal y la fiscal. En este sentido existe toda una regulación sobre el derecho a la privacidad y a la intimidad desde la Constitución de 1857 y con mayor énfasis en la de 1917; en el artículo 16 de la CPEUM dice “nadie podrá ser molestado en su persona, familia,

domicilio, papeles y posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento". Esta regulación de la vida privada se instituyó como una garantía constitucional, pero también existían constituciones locales que incluían instrumentos de protección de la libertad personal. Instrumentos como el *Habeas Corpus* en Aguascalientes, Colima, Guerrero y Puebla (Cienfuegos, 2011), por ejemplo, o el *Habeas Data*[25]

De la misma manera leyes como la de delitos de imprenta consideran como un delito la intromisión en la vida privada; sin embargo, el Código Penal Federal no contempla un tipo penal al respecto; la Ley del Sistema Nacional de Información, Estadística y Geografía contempla los principios de confidencialidad y reserva, y la prohibición de divulgar la información de forma nominativa o individualizada, asimismo prevé el método de disociación, de manera que los datos estén de tal forma que no se pueda identificar a las personas físicas o jurídicas; la ley Federal de Derechos de Autor en su artículo 87 dice que "el retrato de una persona sólo puede ser usado o publicado, con su consentimiento expreso", así como en el artículo 109 se considera que "el acceso a información de carácter privado relativa a las personas contenida en las bases de datos a que se refiere el artículo anterior, así como la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, requerirá la información previa al titular".

La ley para regular las sociedades de información crediticia fue creada en el 2002 y su última reforma realizada en el mes de enero del 2009 se relaciona con los datos personales contenidos en el buró de crédito, que incluye el derecho del cliente a solicitar un reporte que contenga su historial crediticio, y en caso de estar inconforme con los datos ahí contenidos, el titular tiene la posibilidad de presentar una reclamación en los términos que fija el Banco de México. Asimismo, los usuarios pueden acceder a su información que se encuentra en las Sociedades, de la misma manera que las autoridades hacendarias o judiciales; (Instituto de Transparencia e Información Pública de Jalisco, 2010).

[25] Que significa "toma de los datos que están en tu poder y entrégalos al interesado" o "brinda al interesado, mediante certificación, todos los datos o documentos que se encuentran en tu poder que pueda defender él sus derechos en juicio". Para profundizar consultar: Puchinelli, Óscar. 1999. *El Habeas data en Indoiberoamérica*, Bogotá, Temis, p. 296. Citado por Muñoz de Alba Medrano. *Habeas Data*. Página 2, disponible en http://biblio.juridicas.unam.mx/libros/5/2264/4.pdf; "El habeas data no es un derecho fundamental *stricto sensu* sino que se trata de un proceso constitucional. Nos hallamos frente a un instrumento procesal destinado a garantizar la defensa de la libertad personal en la era informática". De Slavin, Diana. 1999. *MERCOSUR: La protección de los datos personales*. Desalma, Buenos Aires. Entonces el *habeas data* es una acción legal que cualquier individuo puede ejercer sobre sus datos personales que obren en un registro, base o banco de datos, de acceder a tal registro para conocer sobre su información, y en su caso, requerir la corrección, modificación o eliminación, según sea el caso.

En las entidades federativas podemos encontrar leyes como la de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, el honor y la propia imagen en el Distrito Federal publicada el 19 de mayo de 2006. Toda esta regulación existía antes de la regulación sobre protección de datos personales en posesión de los particulares. Como se pudo observar, es legislación que va desde leyes secundarias de diversas materias: civiles, fiscales, mercantil, penales, administrativa, entre otras. A esto se debe, en gran parte, la existencia de una regulación sobre privacidad en diferentes ámbitos. Es una regulación y organización de las autoridades de forma sectorial no unificada, donde se protegían los datos personales por medio de la privacidad. Este modelo sectorial no unificado lo adoptó Estados Unidos, como ya se ha analizado, por lo tanto México tenía un modelo similar, que fue cambiando a raíz de la promulgación de la LFTAIPG en 2002, y con mayor fuerza, cuando se regula la protección de datos personales en posesión de los particulares en 2009, siendo oficial en 2010 cuando se publicó la ley en el Diario Oficial de la Federación, y entró en vigor hasta enero del 2012, para dar tiempo de su implementación.

La Ley Federal de Protección de Datos Personales en Posesión de los particulares tuvo como antecedentes diversas iniciativas de ley. La primera data de 2001 —justo cuando se discutía la ley de acceso a la información federal—, fue presentada por el entonces senador Antonio García Torres de la fracción parlamentaria del Partido Revolucionario Institucional. Esta propuesta no se convirtió en ley y el senador volvió a presentar otra propuesta en 2005. Después de su primera propuesta de ley, otros legisladores realizaron sus propuestas respectivas, como el exdiputado Miguel Barbosa, del Partido de la Revolución Democrática, quien la realizó el mismo año (2001), desde la Cámara de Diputados.

Las respuestas a la primera iniciativa se presentaron en seguida por parte del gobierno federal y por parte de las empresas privadas. Se argumentó que la "ley era copia de una antigua ley española de protección de datos personales, ley que había sido muy perjudicial para la empresa, por las restricciones y límites a la libre empresa" (Alfredo Reyes Krafft, entrevista personal, 4 de diciembre de 2014).

Alfredo Reyes Krafft (2014) ha dividido algunas iniciativas de ley en tres tipos: las que proponían un modelo general, las iniciativas del modelo sectorial y las del modelo híbrido o combinado. Esta modalidad permite perfilar objetivos, proceso, intereses y por supuesto modelos para la toma de decisiones y de diseños institucionales y organizacionales de la protección de datos personales. Algunos modelos ya partían de la necesidad de regular de manera conjunta protección de datos personales tanto en el ámbito del sector público como del sector privado, otras

consideraban que la regulación debería ser más permisiva y por lo tanto dividir esta regulación. Finalmente, la regulación híbrida partía de la necesidad de reconocer un contexto diferenciado y con múltiples intereses económicos nacionales e internacionales.

3.1.2.1 Los diseños de protección de datos personales

Los modelos permiten aprehender la realidad de manera sistemática y congruente. En torno a la protección de datos personales podemos identificar tres modelos propuestos en diversas iniciativas de ley específica, iniciativas que van desde 2001 hasta 2008. La propuesta general considera tres modelos básicamente: el general, el sectorial y el híbrido (Reyes, 2014). El modelo de regulación general está basado en la regulación de la Unión Europea, centrado en el dato; tiene alcance para el sector público y privado; protección universal de los datos personales; requiere de una ley general; notificación previa para la recolección de datos personales; aplicación específica de los principios para el tratamiento legal con sólo ciertas excepciones; certidumbre jurídica: mismas reglas para todos los jugadores; los individuos tienen mayor control sobre sus datos; prohibición al flujo transfronterizo, si no hay regulación al menos equivalente en el país receptor; si no hay una ley, deben buscarse otros esquemas de protección –contratos– y un aspecto importante es que debe existir una autoridad supervisora nacional.

El modelo sectorial tiene como ejemplo a Estados Unidos y subyace la teoría de que se debe evitar la sobrerregulación; los mercados se deben autorregular; el Estado debe intervenir únicamente en ciertos casos para proteger a determinadas personas e industrias (financieros, salud, niños); es posible la aplicación limitada de ciertos principios; resulta factible la supervisión sectorial: diferentes autoridades; de otra manera, la autorregulación voluntaria debe darse como una respuesta a las demandas del mercado —posible responsabilidad por una falsa representación y capacidad para limitar los principios que aplicará—. Este modelo está centrado en la persona. Es el modelo sectorial descrito en el capítulo 2 de esta investigación, donde la libertad en el uso de los datos es permisiva si existen mecanismos de consentimiento que permitan justificar el tratamiento de estos.

El modelo híbrido establece derechos, principios y procedimientos de protección; permite a la industria autorregularse con base en las mejores prácticas a nivel internacional, supervisados por una autoridad centralizada y con aplicación general, complementada por prácticas propuestas por sectores específicos de la economía. Asegura un determinado nivel de protección establecido

en la ley, pero los estándares varían de acuerdo con el sector. Existe la posibilidad de confeccionar la protección conforme a los requerimientos de las prácticas de la industria, sin perder en ningún caso la protección al titular de los datos.

A este último modelo Alfredo Reyes Krafft (2014) lo denomina de tercera generación, el cual está basado en principios generales en un mundo global —considerando que la primera generación está basada en la protección a las personas, la segunda generación basada en principios y procedimientos, y la tercera atendiendo a la globalización y las necesidades económicas—. Tres son los elementos de los modelos regulatorios de la protección de datos personales en esta tercera generación: privacidad local, flujo mundial y obligaciones universales. El modelo híbrido retoma experiencias positivas y elimina lo negativo o poco útil (los registros de las bases de datos, por ejemplo), atiende a las nuevas herramientas y sistemas de comunicación, a los conceptos dinámicos, como por ejemplo el computo en la nube o *Cloud Computing*.

El modelo híbrido es un modelo regulatorio que pretende asegurar adaptabilidad y *accountability*. Es un modelo que asegura la privacidad (intercambio de información libre, responsable y segura de la información personal) y que atiendan a la base económica (presunción de protección legal razonable). Este modelo es el producto de "dos modelos que parecían contrapuestos porque los dos buscan la protección de la persona, uno desde un contexto mucho más mercantilista y el otro con un contexto mucho más de protección al propio titular (Alfredo Reyes Krafft, entrevista personal, 4 de diciembre de 2014).

3.1.2.2 Las propuestas en las iniciativas de ley

La primera iniciativa fue "copiada de un antiguo modelo español. En España había un modelo más de comunidad; una regulación que le hizo muchísimo daño a la industria, porque era exageradamente incisiva y era muy restrictiva; la industria promovió en el Congreso una modificación", se adecuó el modelo legislativo, pero García Torres copió el modelo viejo para traerlo y no el nuevo. Entonces el modelo que trajo a México era el modelo restrictivo del cual habíamos tenido referencia que en España en particular había generado mucho daño en la industria y había inhibido el esquema comercial, la promoción comercial, entonces… yo creo que es muy importante la protección de datos, pero también es muy importante el desarrollo económico y en cierto sentido pueden coexistir y hacerlo de una manera ordenada. Ante esta iniciativa que presentó el senador García Torres la industria se unificó. En México lo que hicimos fue, como industria unir esfuerzos con tres grandes empresas: Hewlett Packard, una compañía de seguros muy grande

y Bancomer, nos reunimos porque sentimos que esto podría generar un problema serio para la industria y desde la Asociación Mexicana de Internet buscamos frenar o participar en la negociación de todo esto" (Alfredo Reyes Krafft, entrevista personal, 4 de diciembre de 2014).

En el siguiente cuadro se presentan las propuestas de ley presentadas en materia de datos personales. Propuestas que van desde 2001 hasta 2009 cuando se aprueba la ley que todavía hasta junio de 2015 seguía vigente.

Cuadro 7. Propuesta de Ley sobre Protección de Datos en Posesión de los Particulares.

MODELO	PROPUESTO POR	PARTIDO	FECHA
Primera Iniciativa	*Sen. Antonio García Torres*	*PRI*	*Febrero 14, 2001 y Febrero 2, 2006*
Modelo General	Dip. Luis Gerónimo Barbosa Huerta.	PRD	Septiembre 06, 2001.
	Dip. Jesús Emilio Martínez Álvarez.	Convergencia	Diciembre 01, 2005.
	Dip. Norma Leticia Orozco Torres	PVEM	Febrero 02, 2010.
Modelo Sectorial	Dip. Sheyla Fabiola Aragón Cortés	PAN	Marzo 22, 2006.
	Dip. David Hernández Pérez	PRI	Febrero 23, 2006.
Modelo Hibrido	Dip. Luis Gustavo Parra Noriega	PAN	Octubre 7, 2008.
	Dip. Adolfo Mota Hernández	PRI	Diciembre 11, 2008.
Datos Públicos y Privados	Sen. José Guillermo Anaya	PAN	Diciembre 1, 2009

Fuente. Elaboración propia.

A la primera iniciativa se unió una más del mismo senador, Antonio García Torres. Esta propuesta modificaba el artículo 16 de la CPEUM y tenía como objetivo reconocer el derecho fundamental a la protección de datos personales, sus principios y garantías específicas. Fue presentada el 21 de febrero de 2001 ante el pleno de la Comisión Permanente del Congreso de la Unión. La iniciativa propuso adicionar tres párrafos al artículo 16 de la Constitución[26], que proponían reconocer el

[26] 1). "Toda persona tiene derecho a la protección y al acceso de los datos personales que le conciernen, así como el de acceder a la información de archivos o registros públicos y privados destinados a dar informes, y a conocer el uso o finalidad de tales registros. Los datos se obtendrán y tratarán de modo que no se afecten el honor, la intimidad o cualquier otro derecho de las personas, para fin lícito determinado y con el previo consentimiento, libre e informado de su titular. 2). "No se considera que la obtención y el tratamiento de datos afecta el honor, la intimidad o cualquier otra garantía de la persona a la que conciernen, cuando se realizan atendiendo al interés general del Estado mexicano, a intereses sociales, o con el fin de proteger los derechos fundamentales de terceros por causa legítima. 3). "La persona tiene derecho a la inclusión, actualización, complementación, rectificación, suspensión, reserva y cancelación de los datos que le conciernen". García Torres, Antonio. 2 de febrero de 2006. Minuta

derecho a la protección de datos personales: protección, acceso, y finalidad; así como el tratamiento de los datos con previo consentimiento, libre e informado de su titular. Considerando que no se vulneraban derechos cuando el tratamiento atendía al interés general del Estado mexicano, a intereses sociales o para proteger los derechos de terceros. Asimismo, se reconocían los derechos de inclusión, actualización, complementación, rectificación, suspensión, reserva y cancelación.

La primera iniciativa de protección de datos personales fue presentada el 14 de febrero del 2001 ante la Comisión Permanente del Congreso de la Unión. Ese mismo año —el 6 de diciembre de 2001— fue presentada la iniciativa de Ley Federal de Acceso a la Información Pública Gubernamental —dictaminada y aprobada en la Cámara de Diputados el 24 de abril de 2002 y por la Cámara de Senadores el 30 de abril del 2002. A la par, la Ley de Protección de Datos Personales fue dictaminada y aprobada en la Cámara de Senadores el 30 de abril de 2002, la cual se turnó a la Cámara de Diputados el mismo 30 de abril. En 2001-2002 se presentó la misma situación que en 2014-2015, pues se presentaron la Ley de Protección de Datos Personales por Antonio García Torres y la Ley de Transparencia y Acceso a la Información por el Grupo Oaxaca y el Gobierno Federal. Ambas leyes se pusieron a disposición del proceso legislativo en tiempos similares. Siendo privilegiada para su dictamen y aprobación en ambas cámaras la Ley de Acceso a la Información Pública Gubernamental (García, 2006).[27]

El dictamen negativo de la propuesta fue argumentado considerando que el Congreso no contaba con facultades para legislar en materia de datos personales, que debería ser una ley general. No se hacían menciones específicas sobre las funciones correspondientes al IFAI; no se tomaban en cuenta los avances internacionales y las mejores prácticas; se carecía de estudios sobre impacto económico de la ley; se daba a la persona la facultad de que escogiera a la autoridad competente para conocer el *habeas data;* faltaban referencias para salvar contradicciones con la Ley de Acceso a la Información, y que podría producir efectos contraproducentes sin lograr el objetivo. El mismo senador argumentó que el dictamen de la iniciativa de 2001 estuvo viciado y careció de un debido proceso legislativo (García, 2005).[28]

presentada para la propuesta de la ley sobre protección de datos personales en 2006. Disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/iberoamerica/proyectos/common/pdfs/Proyecto-mexicano.pdf

[27] Las Leyes Generales en materia de Acceso a la Información y Protección de datos Personales fueron presentadas en octubre de 2014 y hasta junio del 2015 sólo la Ley General sobre Acceso a la Información había sido aprobada. Con esta ley también se modificó el nombre del IFAI a INAI (Instituto Nacional de Acceso a la Información Pública y Protección de Datos). En este sentido, se le dio preferencia al tema de Acceso a la Información y se dejó a discusión el tema de Protección de Datos Personales

[28] El día 14 de diciembre de 2005, sin que estuviera listada en el orden del día correspondiente y ya comenzada la sesión plenaria de la Cámara de Diputados del Congreso de la Unión, se solicitó que se incluyera como asunto a

Alfredo Reyes Kraft (2014), quien estuvo presente en las discusiones sobre la ley en materia de datos personales, argumentó que "una ley no puede presentarse dos veces. El problema es que una misma iniciativa de acuerdo con la Constitución no puede ser presentada dos veces al Congreso y en el propio texto de la exposición de motivos ratifica que la vuelve a presentar, entonces lo que se hace es que *tumban* las dos iniciativas en el Congreso", para que luego la presentaran los principales representantes del PRI, PAN y PRD. Los diputados desecharon las dos iniciativas. Luego ocurrió una cuestión interesantísima: él había presentado una reforma al artículo 16 constitucional y era buena reforma, que desecharon los senadores, la modificaron y de la mano los tres partidos más importantes en ese entonces en Cámara presentaron la iniciativa como reforma constitucional. "Quienes presentan la iniciativa de reforma constitucional, fueron el representante del PAN, del PRI y del PRD, y lo único que hicieron fue modificarla para que no quedara huella del antecedente de la propuesta de García Torres. Dicen que hay dos cosas que no conviene saber cómo se hacen: las salchichas y las leyes" (Alfredo Reyes Krafft, entrevista personal, 4 de diciembre de 2014).

"Las iniciativas de García Torres establecían un poder omnímodo para la autoridad, es decir la iniciativa original era que la autoridad tenía casi el poder de hacer y deshacer, era impresionante, entonces como industria estuvimos proponiendo la posibilidad de que existieran dos tipos de autoridades: una autoridad garante y autoridades reguladoras que de alguna manera establecieran la normativa y que la autoridad garante la impusiera. Por otro lado, se estaba en contra de algunos puntos tales como: el consentimiento expreso, las sanciones, la autorización de la autoridad garante para las transferencias internacionales, la creación del registro de base de datos para los particulares, y se proponían los mecanismos de autorregulación similares a los de APEC y la certificación de C.H. Robinson en materia de puerto seguro" (Alfredo Reyes Krafft, entrevista personal, 4 de diciembre de 2014). Estos fueron los puntos donde la industria organizada intervino para detener, modificar y proponer a las iniciativas presentadas.

discutir el dictamen en sentido negativo de la iniciativa, lo cual fue aprobado en votación económica y de manera inmediata se acordó por votación económica discutir en lo general y en lo particular en un solo acto, para que después el dictamen en sentido negativo fuera votado en forma económica por la mayoría de legisladores. Este proceder es contrario no sólo a la práctica parlamentaria, sino también a lo prescrito en la propia normativa que rige las actividades del Congreso, pues el dictamen debió ser distribuido y publicado en la Gaceta Parlamentaria de la Cámara de Diputados para poder ser discutido e, incluso, las votaciones del dictamen debieron ser nominales, no económicas (artículos 20.2 c), y 36.1.c) de la Ley Orgánica del Congreso General de los Estados Unidos Mexicanos y 117, 146, 147 y 148 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos). García Torres, Antonio. 2006. Exposición de motivos. Ley de Protección de Datos Personales. 2 de febrero de 2006

Después de la primera iniciativa presentada por García Torres, vinieron otras propuestas como la de Miguel Barbosa —senador de la república electo para el periodo 2012-2018 y presidente de la mesa directiva del Senado de la República del 2014 al 2015, quien presentó una iniciativa que proponía regular la protección de datos tanto para el sector público como para el privado, de manera conjunta. Una articulación de derechos, sujetos y normativas: para públicos y privados, para personas físicas y cuando fuera pertinente a las personas morales, así como la consideración de los derechos de impugnación de valoraciones, de consulta, de acceso, de ratificación, de cancelación, de oposición y de indemnización. Con la creación de un Registro Nacional de Protección de Datos Personales integrado al Instituto Nacional de Estadística y Geografía.

La siguiente propuesta fue una copia de la iniciativa presentada por Antonio García Torres. Esta iniciativa la presentó Jesús Martínez Álvarez, diputado Federal, en sesión del 1 de diciembre del 2005, ante el Pleno de la Cámara de Diputados (García, 2006: 6 y Krafft, 2014). Iniciativa ante la cual el mismo senador Antonio García Torres respondió presentado nuevamente otra iniciativa de ley. Estas primeras cuatro propuestas forman el primer cuadro de iniciativas y a partir de aquí se da paso a una nueva etapa de propuestas donde la industria agrupada en organizaciones, y en coordinación con algunos diputados, realizaron sus propias aportaciones.

Tanto la primera como la segunda iniciativa de García Torres (2001 y 2006) motivaron y originaron la intervención por parte de la industria organizada. La nueva propuesta que presentó en 2006 originó contrapropuestas entre la industria organizada y algunos diputados federales. "Ante esta iniciativa que presentó el senador García Torres la industria se unificó originalmente con la idea de tres grandes empresas: de Hewlett Packard (HP), de una compañía de seguros muy grande —MetLife— y de Bancomer. Nos reunimos porque sentimos que esto pudiera generar un problema serio para la industria y desde la Asociación Mexicana de Internet (AMIPCI) buscamos, por así decirlo, frenar o participar en la negociación de estas propuestas" (Alfredo Reyes Krafft, entrevista personal, 4 de diciembre de 2014).

"La representación de HP fue Jacobo Esquenazi, la de MetLife Alejandro y Miguel Ángel Flores. Este fue el grupo básicamente quienes estábamos representando a dos grandes organizaciones: La Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI) representada por Alejandro Flores y yo que en ese entonces era presidente de la AMIPCI" (Alfredo Reyes Krafft, entrevista personal, 4 de diciembre de 2014).

Estos representantes de la industria se reunieron para lograr un consenso y tratar de negociar, Alfredo Reyes refiere lo siguiente: "nos reunimos para negociar las fallas que tenía esa normativa a nuestro juicio; nos presentamos al Congreso y nos dicen "ustedes lo único que quieren es utilizar los datos de los particulares, no les interesa la protección de los datos; son representantes de la industria; ustedes lo que quieren o están buscando es puro beneficio económico y poder aprovecharse de los ciudadanos para tener datos y con eso generar ganancias… porque el dato ha tenido o tiene ya un contenido de carácter económico. Entonces ideamos una estrategia que nos diera legitimidad y confianza para negociar en la Cámara de Diputados. Creamos con base en el modelo APEC de privacidad un *framework* de privacidad y un sello de confianza, en donde las empresas se obligaban a seguir ese marco de privacidad de APEC, para proteger los datos de sus potenciales clientes. Alrededor de 400 o 500 empresas acordaron o estuvieron conscientes en firmar y comprometerse aun cuando no existía una obligación legal para ello, formalmente. Esta negociación y la disponibilidad de las empresas para sujetarse a lineamientos internacionales dio cartas y legitimidad para poder negociar en el Congreso, fue difícil, fue muy complejo, pero logramos incidir en el Congreso y tener legitimidad para poder armar todo" (Alfredo Reyes Krafft, entrevista personal, 4 de diciembre de 2014).

Al involucrarse y contar con la posibilidad de negociar, entraron en contacto con algunos legisladores, además de tomar fuerza con la Cámara Internacional de Comercio y con el Consejo Mexicano de Hombres de Negocios. Se empezó a negociar y a trabajar en el modelo de regulación desde el Congreso. "Ya estando en el inicio de la negociación, la manera en que pudiéramos de alguna manera rebatir o minimizar un poquito el impacto de esa normativa en la industria fue presentando una contrapropuesta. ¿Qué hicimos?, el entonces director jurídico de Microsoft, Mauricio Domingo Donovan, en conjunto la diputada Sheila Fabiola Aragón Cortés, hicimos una iniciativa del Congreso, muy al modelo norteamericano, exageradamente contrapuesta al modelo que había presentado el senador Antonio García Torres, entonces la presentamos. La verdad es que fue una iniciativa que tenía fallas de fondo, porque era copia de una normativa americana que era aplicable en sólo un sector en lo particular, pero lo armamos, tratamos de darle forma y posteriormente la corregimos con una iniciativa que presentó el diputado David Hernández Pérez, del PRI" (Alfredo Reyes Krafft, entrevista personal, 4 de diciembre de 2014).

En estas propuestas, los temas de gran importancia y relevancia para la industria organizada fueron "el consentimiento, las sanciones, las competencias de la autoridad garante sobre las transferencias internacionales, el registro de base de datos para los particulares, y los

mecanismos de autorregulación similares a los de APEC y la certificación de C.H. Robinson en materia de puerto seguro. Ellos estaban en contra de que para tratar los datos personales se necesitara la autorización expresa del titular de los datos personales; consideraban que las sanciones no deberían ser un aliciente económico para la propia autoridad garante —es decir que no fuera un sistema de financiamiento para la autoridad garante—. Asimismo, se luchó por contravenir la idea de que la autoridad garante tuviera que autorizar la transferencia internacional de datos personales, para dejar la autorización en manos de su titular. Y algo que se promovió fuertemente fueron los mecanismos de autorregulación (Alfredo Reyes Krafft, entrevista personal, 4 de diciembre de 2014).

Luego de las contrapropuestas de la industria organizada vinieron otras iniciativas más. Pasaron varios años de negociación donde participaban diputados federales, organizaciones empresariales, el IFAI, la Secretaría de Economía, agencias internacionales de protección de datos como la de España, y en cierta medida las pugnas de las entidades federativas. Se lograron primero dos iniciativas de reforma constitucional. La del artículo 16 constitucional y la del artículo 73. La primera adicionó dos párrafos donde se reconocía la protección de los datos personales como garantía constitucional, además de los derechos de Acceso, Rectificación y Oposición. Así como los respectivos límites de esta protección. En el artículo 73 constitucional se facultó al Congreso de la Unión para legislar en materia de protección de datos personales en posesión de los particulares.[29]

Las dos iniciativas que se presentaron posteriormente fueron las que terminaron por fusionarse y lograron acuerdos entre los diferentes actores políticos y económicos para aprobar la ley Federal de Protección de Datos Personales en Posesión de los Particulares. Estas iniciativas son las siguientes.

3.1.2.3 El diseño hibrido de la protección de datos

Después de varios años de negociación, con las reformas constitucionales, en 2008 se presentaron dos iniciativas más: la del diputado Luis Gustavo Parra Noriega, del PAN, del 7 de octubre de 2008, y la del diputado Adolfo Mota Hernández, del PRI, en diciembre 11 del 2008. En el inter de

[29] La iniciativa del Artículo 73 constitucional fue presentada por el diputado Gustavo Parra, turnada a la Comisión de Puntos Constitucionales de la Cámara de Diputados; dictaminada en sentido positivo y aprobada en esa Cámara el jueves 20 de septiembre de 2007. Aprobada en minuta el 5 diciembre del 2008 por el Senado de la República, publicada en el Diario Oficial de la Federación el día 30 de abril de 2009

la discusión de estas iniciativas aparecieron los Estándares internacionales de protección de datos personales y privacidad, también conocido como la Resolución de Madrid, el 5 de noviembre del 2009.

La iniciativa del diputado Gustavo Parra consideró la protección de datos personales sólo en posesión de los particulares, asimismo la definición de dato personal, se diferencia entre datos personales sensibles y datos personales de identificación; tratamiento de datos y disociación; por lo que respecta al principio del consentimiento, se establece la obligación consistente en que todo tratamiento de datos personales requiere del consentimiento de su titular; concretamente en lo referente a datos sensibles se prevé que ninguna persona está obligada a proporcionar sus datos personales sensibles, únicamente cuando medie un consentimiento expreso, informado y entendible del titular de los mismos. Se manifestó el tratamiento informado mediante el aviso de privacidad, así como principios de calidad, seguridad; los derechos de Acceso, Rectificación, Cancelación y Oposición; un proceso de solicitud consistente con la intervención de la autoridad garante si no se da solución a la solicitud del particular; se previó el proceso de revisión; infracciones y sanciones para quienes infrinjan la ley, así como la creación de una Comisión Nacional de Protección de Datos Personales con la naturaleza jurídica de un organismo descentralizado de la Administración Pública Federal, no sectorizado, dotado de personalidad jurídica y patrimonio propio; contando con plena autonomía técnica y de gestión, así como para dictar sus resoluciones.

La propuesta de Adolfo Mota Hernández también consideró como sujetos obligados a las personas físicas o morales de carácter privado; consideraba como exclusión de los sujetos regulados a los poderes Ejecutivo Federal, Legislativo y Judicial, organismos autónomos, tribunales, sindicatos, sociedades de información crediticia y las asociaciones religiosas. No consideraba como datos personales el nombre, puesto, la dirección y el teléfono de un empleado, prestadores de servicios o miembros de una organización, así como la información que una persona hace pública de forma deliberada, o permite que sea hecha pública, o que es obtenida de registros públicos u otras fuentes accesibles al público en general de conformidad con las leyes, aquellos datos que obran o que son utilizados en el ejercicio de actividades exclusivamente personales o domésticas; se prevén para organizaciones civiles y gubernamentales —nacionales o extranjeras— esquemas de autorregulación para complementar la ley; el principio de aviso informado del tratamiento de datos; los principios de aviso, calidad, licitud, acceso, corrección, seguridad, custodia y consentimiento; asimismo, le otorga un aspecto importante al aviso de privacidad, se

excluye a los datos sensibles considerando que para tratarlos se deberá tener consentimiento previo del titular sólo para divulgación o fines secundarios, el consentimiento para tratamiento de datos sensibles puede no ser necesario; establece los principios de acceso y corrección, así como la creación del Instituto de Protección de Datos Personales como organismo descentralizado dependiente de la Secretaría de Economía, con personalidad jurídica y patrimonio propio. Prevé un procedimiento administrativo de protección de datos y estableció multas que van de 100 a 500 días de salario mínimo general diario en el Distrito Federal o de 500 a 1000 días, según la infracción, sanciones menores a las que propuso Gustavo Parra.[30]

Al interior de la Cámara de Diputados existía desconocimiento de la materia, sin embargo, diputados como Gustavo Parra, que habían tenido un acercamiento al tema de Acceso a la Información y protección de datos personales desde las propuestas que realizó en el Estado de México, fueron posicionando el tema: "El cabildeo estuvo presidido por el diputado Adolfo Mota como interlocutor del PRI y por parte del PAN contamos con el apoyo del diputado Diódoro Carrasco para desarrollar la iniciativa y empujarla. Acordamos cada uno desarrollar una propuesta; se presentan las propuestas y todo el cabildeo se realiza en la Comisión de Gobernación" (Gustavo Parra Noriega, entrevista personal, 24 de noviembre del 2014).

También "se contó con el apoyo de la fundación Miguel Estrada; con la aprobación en ese entonces de la vicecoordinadora jurídica del grupo parlamentario de Acción Nacional la senadora Pilar Ortega, con Héctor Larios que era el coordinador de los diputados. Este fue un tema que fuimos introduciendo en la agenda, fuimos poniéndolo como un tema que debía estar en la agenda política, en la agenda legislativa y que se tenía que avanzar en el diálogo con los partidos y poco a poco avanzó y logró resultados" (Gustavo Parra Noriega, entrevista personal, 24 de

[30] La propuesta de Gustavo Parra para el artículo 56. Las infracciones a la presente Ley serán sancionadas por la Comisión con: I. La obligación de que el particular lleve a cabo los actos solicitados por el titular, en los términos previstos por esta Ley, tratándose de los supuestos previstos en las fracciones I y II del artículo anterior; II. Multa de 100 a 2000 días de salario mínimo vigente en el Distrito Federal, en los casos previstos en la fracción III, V, IX y X del artículo anterior; III. Multa de 200 a 5,000 días de salario mínimo vigente en el Distrito Federal, en los casos previstos en las fracciones IV, VI, VII, VIII del artículo anterior. IV. En caso de que persistan infracciones a la presente Ley, se impondrán nuevas multas por cada día que transcurra sin que se obedezca el mandato respectivo, hasta por 200 días de salario mínimo vigente en el Distrito Federal. Adolfo Mota: artículo 47. En los supuestos descritos en las fracciones III, IV, VII y VIII del artículo 46, el Instituto aplicará al infractor, dependiendo de las circunstancias del de comisión de la infracción, y la reincidencia en su caso propio infractor, un apercibimiento o multa por evento hasta por el equivalente de 100 a 500 días de salario mínimo general diario vigente en el Distrito Federal al momento de la comisión de la infracción. En los supuestos previstos en las fracciones I, II, V, y VI del artículo 46, el Instituto aplicará al infractor, dependiendo de las circunstancias de comisión de la infracción, y la reincidencia en su caso del propio infractor, la sanción de apercibimiento o multa hasta por el equivalente de 500 a 1000 días de salario mínimo general vigente en el Distrito Federal al momento de la comisión de la infracción.

noviembre del 2014).

Esta discusión en el Congreso nuevamente tuvo como partícipes a miembros de las organizaciones empresariales e industriales, tales como la Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI), entonces representada por Jacobo Esquenazi. "Ellos estuvieron atentos a ese proceso, buscando que la ley no fuera un obstáculo para el tema de las nuevas tecnologías. También participó Alfredo Reyes Krafft de AMIPCI (Asociación Mexicana de Internet)[31]. Por el lado del IFAI quien nos acompañó mucho en esta propuesta fue Lina Ornelas y en su momento el propio Alonso Lujambio, nos ayudó bastante a que esto pudiera ser una realidad, y luego hicimos foros internacionales donde trajimos al Dr. José Manuel de Frutos Gómez, de la Comisión Europea,[32] él estuvo también muy atento a la propuesta de México, participaron representantes de COPARMEX, de la Secretaría de Economía. También había quienes a lo mejor preferían que no hubiera ley, porque estaban en el mejor de los mundos, nadie los regulaba, pero era necesario avanzar, teníamos una laguna de más de 25 años en el tema (Gustavo Parra Noriega, entrevista personal, 24 de noviembre del 2014).

El IFAI acompaño las discusiones de las diversas leyes de protección de datos personales, pero lo realizó con mayor énfasis a partir de 2007. "De 2007 a 2009 hubo un impulso total de este Instituto, al menos, de la Dirección General de Clasificación y Protección de Datos a cargo de Lina Ornelas, y por supuesto con el apoyo y con la autorización de los mandos superiores. El acercamiento era principalmente técnico, con recomendaciones, opiniones basadas en el Derecho Comparado y en la experiencia propia adquirida manejando los datos personales en posesión del sector público. Así participábamos en algunas reuniones que nos permitían el acercamiento con el presidente de la Comisión, los representantes de los diputados, los propios diputados, los integrantes de las comisiones que en su momento les tocaría llevar proyecto al pleno y eventualmente votar. El acercamiento del IFAI fue así, con la Comisión, con asesores o con diputados. Dábamos puntos de vista técnicos, pues al final justo eran meros insumos los que proveíamos porque las decisiones pasaban por los propios diputados. Esa fue la manera en cómo intervinimos (Edgardo Martínez, entrevista personal, 24 de noviembre de 2014).

La discusión final de la ley no sea realizó en la LX legislatura, en la que tuvo origen. Su discusión y dictamen fueron concluidos en la LXI legislatura —del 1 de septiembre de 2009 al 31

[31] Para 2018 AMIPCI ya había cambiado su denominación a Asociación de Internet. Para más información, consultar: Asociación de Internet, 2018. Disponible en: https://www.asociaciondeinternet.mx/es/

[32] Encargado de la Unidad de Protección de Datos Personales, de la Dirección General de Justicia, Libertad y Seguridad de la Comisión Europea.

de agosto de 2012—, donde el diputado Javier Corral Jurado del PAN fue quien tomo las iniciativas para darles continuidad. El dictamen se dejó aprobado en la comisión de gobernación, pero ya no se pudo subir al pleno por el tiempo ocupado en la reforma del artículo 73 constitucional y el problema de la influenza H1N1, por lo tanto, en 2010 con la nueva legislatura, la LXI federal, se trabajó con Javier Corral quien presidia la comisión de gobernación. Él tomó el tema, lo condujo y finalmente se pudo aprobar en 2010. Esta legislación federal le dio un desarrollo y una fundamentación muy clara al derecho de protección de datos en el ámbito privado (entrevista personal a Gustavo Parra, 24 de noviembre de 2014)

En la fase final en la Comisión de Gobernación, que presidía el diputado Javier Corral Jurado (PAN) las negociaciones continuaron en reuniones de trabajo, eventos y audiencias públicas. El 03 de marzo de 2010 se convocó a una reunión de trabajo en audiencia pública con miembros de Consejo Coordinador Empresarial (CCE) quienes plantearon algunas observaciones al proyecto de dictamen de la ley. A esta audiencia del 4 de marzo de 2010 asistieron como ponentes Luis Miguel Pando Leyva, director general del CCE; Eduardo Amerena Lagunes de la Asociación de Bancos de México (ABM); Ricardo Islas Mondragón de CANACO Ciudad de México; Miguel Ángel Flores de MetLife; Jacobo Esquenazi representando a CANIETI. Asistieron sólo como participantes Fernando Coronel Landa (CCE); Ricardo Araiza Celaya (ABM); Carla Salcido (ABM); Ricardo Navarro Benítez (CONCANACO); Roberto Lazo de la Vega (AMIS); Mónica Leñero Álvarez (ANTAD); Alfredo Reyes Kraft (AMIPCI); Arie Ellstein Cimet (MetLife); Graciela Gutiérrez Garza (CANIETI); Alejandro Martínez (AMITI); Armida Sánchez (Microsoft); Adolfo Hegewish (HP); Mariana Cordera, asesora, y Luis Felipe Briseño (COPARMEX) (Cámara de Diputados, LXI legislatura, Comisión de Gobernación, 2010)

Los temas de la discusión fueron: consentimiento, permiso de privacidad, sanciones, multas, definición *vs.* mención específica de datos sensibles, y las facultades de la autoridad reguladora. Miguel Pando argumentaba que el daño mayor sería para las pequeñas empresas; se buscaba una ley que procurara involucrar el conocimiento y la valoración de las experiencias internacionales. Manifestaba la preocupación de que se considerara al IFAI para ocupar la posición del órgano regulador, pues el IFAI tenía suficiente prestigio en el trabajo con datos públicos, y trabajar con datos privados podría pervertir su función. El consenso de las organizaciones del sector empresarial es que debería haber una sola entidad reguladora para el tema de los datos personales.

Por su parte, los comentarios de Eduardo Amerena Lagunes, de la Asociación de

Bancos de México, giraron en torno a tres aspectos: el consentimiento, la definición de la información considerada como sensible, y el IFAI como órgano garante. Puntualizó que "pedir el consentimiento previo al titular de los datos personales para usar sus datos no sensibles, a efecto de que éstos puedan circular causaría que el mercado nacional dejara de funcionar; se estaría promoviendo que las empresas que se dedican a este servicio a los productores de bienes y servicios migraran del país, se irían a un lugar donde no tuviesen esta regulación y entonces sí podríamos estar ante la presencia de un daño a la economía. Señaló que los datos personales no sensibles permiten que los mercados funcionen, ya que aquellas personas productoras de bienes y servicios que no tienen los recursos para anunciarse en los medios de comunicación electrónicos o escritos recurren al telemercadeo, a las ofertas por teléfono". Sobre los datos sensibles dijo que es preferible que se señalen expresamente; "que se termine con el subjetivismo en la ley", en lugar de que sólo se definan. De igual forma advirtió que implicar al IFAI en una actividad que tiene que ver con mercados y con operación de instrumentos al servicio de la producción o de la prestación de servicios lo desviaría de las funciones para las que fue creado; lo va a desnaturalizar, argumentaba. Por ello, propuso que fuera la Secretaría de Economía la que se encargara de ser el órgano regulador, "hay maneras de que un ente regulador sea la cabeza de esto y es necesario que sea una dependencia acorde a esta función que podría ser la SE, así lo planteamos desde el principio" (Amerena Eduardo, intervención en Cámara de Diputados, 2010)

Además de la audiencia pública con el CCE también se realizaron audiencias con el IFAI, en las que participaron Jacqueline Peschard, entonces comisionada presidenta del IFAI; los comisionados María Marván Laborde, María Elena Pérez-Jen Zermeño y Ángel Trinidad Zaldívar, así como Alejandro del Conde Ugalde, Secretario Ejecutivo y Lina Ornelas Núñez, Directora General de Clasificación y Datos Personales. Ellos manifestaron la importancia de contar con una ley, así como la necesidad de aclarar temas como el consentimiento, las sanciones o multas, la definición de datos sensibles y la autoridad garante. Sobre el consentimiento se partía de la idea de aclarar entre tácito y expreso, así como su relación con el aviso de privacidad; sobre la definición de datos personales sensibles se discutió ampliamente, llegando a la consideración de que su definición debería tener dos apartados: uno que considerara la afectación a la intimidad y la otra parte que enunciara los datos sensibles que se prevén en organismos internacionales, considerados como los más comunes o fundamentales, sin lo cual se restringe la protección. Sobre las sanciones se aclaró que son acordes con las prácticas nacionales e internacionales, pero que además se contempla el tipo de empresa y el tipo de base de datos a sancionar. Finalmente se trató el tema

de la autoridad reguladora, donde se discutió si el IFAI sería la autoridad garante o no. Este tema lo trataremos en el siguiente apartado (Cámara de Diputados, Comisión de Gobernación, 2010).

Estas audiencias, el foro de datos personales[33], los compromisos internacionales con APEC, la OCDE, ONU y el TLC,[34] los compromisos nacionales enmarcados en el Plan Nacional de Desarrollo[35] y la propia necesidad del IFAI de regular la protección de datos personales en posesión de los particulares, dieron origen a la versión final del dictamen de la ley. En este sentido, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares se publicó el 5 de junio de 2010 en el Diario Oficial de la Federación, entrando en vigor el día siguiente a su publicación, pero surtiendo efectos a partir de enero del 2012.

Esta ley quedó, de la siguiente manera. La ley protege a la persona física titular de los datos; los datos sensibles son definidos con dos apartados: la definición general y la particular —artículo 3 fracción VI—; se consideran dos tipos de consentimiento: el tácito y el expreso.

- **El consentimiento tácito** es que "el titular consiente tácitamente el tratamiento de datos, cuando habiéndose puesto a su disposición el aviso de privacidad y no manifieste su oposición".
- **El consentimiento expreso** será cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o mediante cualquier otra tecnología, o por signos inequívocos (artículo 8). El consentimiento expreso se considera verbal o escrito.

[33] Cámara de Diputados, 2010. Retos y perspectivas legales en materia de protección de datos personales. Convocado por la Comisión de Gobernación de la Honorable Cámara de Diputados, LXI Legislatura. Disponible en: http://www3.diputados.gob.mx/camara/001_diputados/010_comisioneslxi/001_ordinarias/020_gobernacion/013_ley_federal_proteccion_datos_personales/00001_discursos

[34] El Diputado Adolfo Mora Hernández indica en su propuesta de ley: "se ha buscado un apego a los principios internacionales de los que México es parte, principalmente APEC y OCDE", con el fin de dar cumplimiento a los compromisos contraídos por México." (pág. 12). Esto quiere decir que al ser México una economía parte de APEC tenía que adoptar medidas para cumplir con el Marco de Privacidad de APEC. También sus compromisos con los lineamientos de la OCDE, ya que México es también un Estado miembro de la OCDE. Incluso diría que como socio comercial de la Unión Europea, en virtud del acuerdo global del año 2000, donde México se comprometía también con esta última a cooperar en materia de protección de datos personales (artículo 41). A lo anterior, se le puede sumar el hecho de que México, después de haber publicado la LFPDPPP, ya ha manifestado su intención de firmar el Convenio 108 del Consejo de Europa (Comunicado disponible en: http://comunicacion.senado.gob.mx/index.php/informacion/boletines/14365- proponen-que-mexico-firme-convenio-108-del-consejo-de-europa-sobre-proteccion-de-datos.html). Son, por lo tanto, varios los compromisos que México ha ido adquiriendo a nivel internacional a lo largo del tiempo y, además, ahora tendrá que seguir trabajando en la materia si firma el Convenio del Consejo de Europa, y aun no firmándolo, para garantizar un alto nivel de protección de datos. Dicho nivel alto de protección incluso con una visión internacional (entrevista con Miguel Recio Gayo, 19 de noviembre de 2014).

[35] En el Plan Nacional de Desarrollo está prevista la emisión de una ley de protección de datos; además tenemos compromisos internacionales con la OCDE, con la ONU, con el Tratado de Libre Comercio de la Unión Europea y con la Ley Iberoamericana para que nosotros tengamos una ley y podamos cubrir los estándares que se tienen en estas organizaciones.

- El verbal es cuando el titular lo externa de manera oral de manera presencial, o mediante el uso de cualquier tecnología que permita la interlocución oral" (artículo 18), y
- El escrito es cuando se otorgó mediante un documento con su firma autógrafa, huella dactilar o cualquier otro mecanismo autorizado por la normativa aplicable, por ejemplo, en el entorno digital la firma electrónica, o cualquier otro procedimiento que permita identificar al titular y recabar su consentimiento —artículo 19 del Reglamento—" (Recio, 2013: 17).

La autoridad garante o de control quedó conferida al IFAI (a partir del 2015 INAI), y como autoridades reguladoras se encuentran la Secretaría de Economía, las Sociedades de Información Crediticias (como excepción a la ley) y toda aquella dependencia que en el ámbito de sus propias atribuciones regule datos personales —artículo 40 de la Ley—. Las sanciones o multas se prevén en el artículo 61 de la fracción I a la IV, los apercibimientos, multas de 100 a 160 mil días de salario vigente; multas de 200 a 320 mil días de salario mínimo vigente en el Distrito Federal. Las sanciones podrán incrementarse hasta el doble de los montos establecidos, cuando sean datos sensibles.

Esta es la manera como se diseñaron las instituciones hasta 2015 de protección de datos personales. En el siguiente apartado se analiza la manera en cómo se diseñó la autoridad garante de la protección de datos personales en México. Es importante recordar que la Ley General en la materia no forma parte propiamente del análisis de esta investigación, sin embargo, se toma en cuenta en las conclusiones de este trabajo.

3.2 Diseño de la autoridad garante

En México se decidió asignar la función de garante de la protección de datos personales al Instituto Federal de Acceso a la Información Pública Gubernamental (IFAI) en 2010, aunque es importante resaltar que esta institución ha tenido cambios considerables. Actualmente (2019) se denomina Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Por lo que inició siendo autoridad en materia de acceso a la información y posteriormente se la asignó ser garante de la protección de datos personales en posesión del sector público y del sector privado.

Para conocer por qué es la autoridad garante veamos cómo se decidió que fuera el IFAI

(ahora INAI) la principal autoridad garante. Es la principal porque existen otras autoridades que tienen competencias específicas sobre la protección de datos personales, como por ejemplo la Secretaría de Economía, la Procuraduría del Consumidor, las Sociedades de Información Crediticia. A estas autoridades se les llama autoridades reguladoras. Incluso los propios tribunales y la Suprema Corte de Justicia de la Nación tienen en su ámbito de competencia funciones en materia de protección de datos personales.

El Instituto Federal de Acceso a la Información Pública Gubernamental (IFAI) fue creado en 2003 por decreto presidencial de Vicente Fox Quesada como un organismo público descentralizado de la administración pública, con patrimonio propio. El IFAI inicio tempranamente sus relaciones con diversas agencias de protección de datos personales, a raíz de que se le facultó para proteger en el sector público primero, luego en el privado los datos personales. La Agencia Española de Protección de Datos Personales fue un aliado importante. José Luís Piñar Mañas (ex director de la Agencia) visitó al IFAI en 2003: "de mis primeras visitas oficiales como director de la agencia fue a México. En el año 2003 estuve en México cuando estaba recién constituido el IFAI. Recuerdo que fui a la sede inicial del IFAI, en Av. Insurgentes, en un tercero o cuarto piso, un piso muy pequeño. Estaba como presidenta la comisionada María Marván; eran muy pocas personas las que constituían el IFAI" (José Luis Piñar, entrevista personal, 2 de octubre de 2014)[36].

El diseño organizacional del IFAI tuvo cambios significativos. Primero como órgano desconcentrado, luego autónomo y posteriormente una ampliación de sus atribuciones con la aprobación de las leyes generales en materia de acceso a la información y la respectiva en datos personales.

3.2.1 Autoridad garante en las propuestas de ley

En su generalidad las iniciativas de ley sobre protección de datos personales consideraron una autoridad diferente al IFAI como órgano garante. Las iniciativas presentadas tuvieron las siguientes propuestas respecto a la autoridad garante para la protección de datos personales en México.

[36] El IFAI (INAI) ha tenido tres sedes: la primera en Av. Insurgentes, la segunda en Av. México, en Coyoacán, y finalmente en Avenida Insurgentes Sur 3211, igual en Coyoacán. Estos cambios representan modificaciones sustanciales relacionadas con su estructura, funcionamiento, competencias y facultades. El cambio que presentó de encontrarse en avenida México a Insurgentes sur 3211 fue la entrada en vigor de la Ley de Protección de Datos Personales en Posesión de los Particulares. Para 2015, con autonomía y con la previsión de las leyes generales en materia de acceso a la información y protección de datos personales, su prepuesto y su nombre, su estructura, sus competencias, funciones y facultades se vieron modificadas.

Cuadro 8. Autoridades garantes según propuestas de ley

DIPUTADO (A) Y GRUPO PARLAMENTARIO	INICIATIVA DE LEY	AUTORIDAD PROPUESTA	TIPO DE AUTORIDAD
Sen. Antonio García Torres (PRI)	15 de febrero de 2001	Instituto Federal de Protección de Datos Personales	Organismo público descentralizado de la administración pública federal, con personalidad jurídica y patrimonio propios
	2 de febrero de 2006	Instituto Federal de Acceso a la Información Pública.	IFAI
Dip. Miguel Barbosa (PRD)	30 de abril de 2002	Registro Nacional de Protección de Datos	Ente integrado al Instituto Nacional de Estadística, Geografía e Informática.
Dip. Jesús Martínez Álvarez (Convergencia)	1 diciembre de 2005	Al Instituto Federal de Protección de Datos Personales	Contará con 3 comisionados exclusivamente sobre protección de datos.
Dip. David Hernández Pérez (PRI)	23 de febrero de 2006	Instituto Federal de Acceso a la Información Pública.	IFAI
Dip. Sheyla Aragón Cortés (PAN)	22 de marzo de 2006	Instituto Federal de Acceso a la Información Pública	IFAI
Dip. Luis Gustavo Parra Noriega (PAN)	7 de octubre de 2008	Comisión Nacional de Protección de Datos Personales	Organismo descentralizado de la Administración Pública Federal, no sectorizado, dotado de personalidad jurídica y patrimonio propio; contando con plena autonomía técnica y de gestión, así como para dictar sus resoluciones.
Dip. Adolfo Mora Sánchez (PRI)	11 de diciembre de 2008	El Instituto de Protección de Datos Personales,	Organismo descentralizado dependiente de la Secretaría de Economía, con personalidad jurídica y patrimonio propio.

Fuente. Elaboración propia.

La primera iniciativa de ley con el exsenador Antonio García Torres (2001) contemplaba una agencia especializada para la protección de datos personales, pero en su segunda propuesta contempló al IFAI dadas las críticas y las presiones a las que se vio orillado tanto por miembros de la Cámara de Diputados, como del gobierno. Al final dijo que lo más importante era contar con una legislación sobre la materia, pues la protección a las personas en el manejo de sus datos era necesaria y fundamental. Su propuesta de una agencia independiente venía influenciada por la regulación española que contempla una autoridad especializada, independiente y con la capacidad técnica para resolver asuntos sobre la protección de datos personales.

La propuesta del exdiputado Miguel Barbosa (2002) consideró como autoridad en materia de protección de datos personales al Instituto Nacional de Estadística, Geografía e Informática,

esta área sería denominada Registro Nacional de Protección de Datos. Autoridad que estaría encargada de coadyuvar en el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial con los derechos de información, acceso, rectificación, oposición y cancelación de datos. En este registro se prevé la inscripción de ficheros de las entidades de los poderes de la unión y los de titularidad privada. Así como realizar un censo de archivos, registros o bancos de datos regulados por la ley y mantener el registro permanente y actualizado de los mismos.

La propuesta del diputado Jesús Martínez Álvarez (2005) no era muy clara porque hablaba de un Instituto Federal de Protección de Datos Personales, pero también en el artículo sobre control de datos personales consideraba que el organismo responsable debería ser el que la Ley de Acceso a la Información estableciera y que esta autoridad debería contar con tres comisionados exclusivamente relacionados a la protección de datos personales. Luego vienen dos propuestas que contemplan al IFAI como autoridad garante, las propuestas de David Hernández Pérez (PRI, 2006) y de Sheyla Aragón Cortés (PAN, 2006). Ambos consideran que el IFAI es el organismo público con la capacidad técnica, con experiencia suficiente para hacerse cargo tanto del acceso a la información como de la protección de datos personales. "Si bien es cierto que el Instituto Federal de Acceso a la Información Pública, creado por virtud de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, es por definición la institución a cargo de la detentación y manejo de información por parte del sector público y no de los particulares, también lo es que la exigencia de razones presupuestarias, obligan a esta soberanía a tener en cuenta la conveniencia de aprovechar las instituciones existentes para dotar de eficacia al marco legal propuesto, y que sea el Instituto quien tenga las facultades para sancionar la eventual violación de las normas de privacidad en que pudieren incurrir los sujetos obligados" (Aragón, 2006). La narrativa final fue contundente, una restricción económica sería le motivo de la balanza a favor del IFAI.

3.2.2 Elección de la autoridad garante

Las iniciativas que se fusionaron fueron la de Gustavo Parra Noriega (2008) y la de Adolfo Mota (2008), ambos contemplaban una autoridad diferenciada. La propuesta de Gustavo Parra Noriega establecía como autoridad administrativa en la materia a la Comisión Nacional de Protección de Datos Personales con la naturaleza jurídica de un organismo descentralizado de la

Administración Pública Federal, no sectorizado, dotado de personalidad jurídica y patrimonio propio, contando con plena autonomía técnica y de gestión, así como para dictar sus resoluciones.

Dentro de las atribuciones estaban: "la promoción y protección de los datos personales en posesión de particulares; el desarrollo, fomento y difusión de análisis, estudios e investigaciones en materia de protección de datos personales en posesión de particulares; el establecimiento de los lineamientos que en materia de seguridad en el tratamiento de los datos personales deban observar los particulares; la emisión de las disposiciones necesarias para la operación, funcionamiento y control del registro de bases de datos previsto en la ley; la difusión de los compromisos asumidos por el Estado mexicano en los instrumentos; procurar la solución de las diferencias entre los titulares de datos personales y los particulares; elaborar el Programa Institucional en materia de Protección de Datos Personales en posesión de particulares; conocer y resolver los procedimientos de declaración de infracción administrativa; resolver los recursos de revisión interpuestos en contra de sus resoluciones, así como imponer las sanciones correspondientes" (Parra, 2008)

En la iniciativa de Gustavo Parra (2008) se propone que la Administración de la Comisión corresponda a la Junta de Gobierno y a la Presidencia de este, previéndose que la Junta de Gobierno esté integrada por cinco representantes de diversas Secretarías de Estado relacionadas con el tema de la protección de datos personales y el presidente de la Comisión, quien la presidiría. Además, con la finalidad de que la Junta de Gobierno tomara sus decisiones apoyada de la experiencia y conocimiento de todos los sectores involucrados en el tema, en su conformación se preveía que pudieran ser invitados a sus sesiones representantes de los sectores económico y social, así como de universidades de educación superior o de organizaciones civiles, quienes asistirían con derecho a voz, pero no a voto.

También su iniciativa previó la creación de la contraloría, órgano de control interno, al frente de la cual estaría la persona designada en los términos de la Ley Orgánica de la Administración Pública Federal. Asimismo, propuso que tuviera un Comisario Público propietario y un suplente, designados por la Secretaría de la Función Pública, quienes ejercerían sus funciones de acuerdo con las disposiciones legales aplicables. En cuanto a la estructura, funcionamiento, operación, desarrollo y control la Comisión se regiría por lo dispuesto la ley de datos personales y también le serían aplicables las disposiciones contenidas en la Ley Federal de Procedimiento Administrativo, en lo que no se oponga a la misma; y las relaciones de trabajo del organismo y su personal, se regirían por la Ley Federal del Trabajo, reglamentaria del Apartado

"A" del artículo 123 de la Constitución Política de los Estados Unidos Mexicanos.

Cabe señalar que no pasó inadvertido en esta propuesta el deber jurídico previsto en el artículo 18 de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, el cual señala que, ante toda propuesta de aumento o creación de gasto del proyecto de Presupuesto de Egresos, deberá agregarse la correspondiente iniciativa de ingreso distinta al financiamiento o compensarse con reducciones en otras previsiones de gasto. Al respecto, Gustavo Parra (2008) dio como argumento que la protección y satisfacción de nuevos derechos y necesidades por parte del Estado, que van surgiendo por virtud del natural dinamismo social y tecnológico, y no se deben limitar por cuestiones presupuestales, sin embargo, sometió al análisis presupuestario su iniciativa, apoyando su argumento en las posibles entradas de recursos al Instituto, vía las sanciones de naturaleza económica, lo que ayudaría a la obtención de los recursos económicos necesarios para el funcionamiento y operación del mismo.

La propuesta de Adolfo Mota (2008) proponía la creación del Instituto de Protección de Datos Personales, autoridad administrativa encargada de la aplicación de esta ley, como un organismo descentralizado dependiente de la Secretaría de Economía, con personalidad jurídica y patrimonio propio, el cual tendría las siguientes facultades —artículo 37—: I. Interpretar en el orden administrativo esta ley; II. Conocer y resolver los procedimientos administrativos de protección de datos personales interpuestos; III. Orientar y asesorar a los particulares acerca del derecho a la protección de datos personales y su procedimiento; IV. Elaborar y difundir estudios sobre la protección de datos personales; V. Proporcionar apoyo técnico a los responsables que lo soliciten, para el cumplimento de las obligaciones establecidas por esta Ley; VI. Vigilar el cumplimiento de las disposiciones de esta Ley y en su caso, determinar las sanciones correspondientes, y VII. Representar a México en los foros internacionales en la materia.

Como se puede observar de todas las iniciativas de ley sólo dos contemplaban al IFAI, aunque sí se incluye la segunda propuesta del exsenador García Torres tres serían las iniciativas que contemplaban al IFAI como autoridad garante. ¿Cómo se logró que fuera el IFAI la autoridad garante si la mayoría de las propuestas contemplaban a una autoridad diferente? Dice el Dr. José Luis Piñar, exdirector de la Agencia Española de Protección de Datos Personales, que al iniciar su gestión él empezó a tener contacto con otras agencias encargadas similares en otros países.

El director de la Agencia Española de Protección de datos detectó que México era y es un país muy relevante en América Latina, y que podría ser un gran referente tanto en materia de Transparencia, como en la de protección de datos personales. México dedicaba en su legislación

una parte a la protección de datos, así que la Agencia Española se dio cuenta de que "podía ser y debía ser muy importante impulsar el tema y colaborar. "En la visita que hice a México no sólo estuve en el IFAI, sino también estuve en el Banco de México, porque entonces había una regulación de ficheros de burós de crédito y el Banco de México tenía una importancia relevante en estos temas. Mantuve reuniones con el Senador García Torres y con algunas personas más del ámbito de la política de varios partidos; con el Instituto Federal Electoral porque es quien llevaba el registro electoral, una de las más importantes bases de Datos" (José Luis Piñar, entrevista personal, 2 de octubre de 2014). La importancia de México en la región Iberoamérica y en América Latina impulsaron esta cooperación. A partir de esta promoción internacional del derecho a la protección de datos personales impulsada por la Agencia Española, México empezó primero a profundizar en el tema en el sector público e impulsar la regulación en el sector privado.

De ahí deriva la importancia del IFAI en materia de protección de datos personales. Sus relaciones con otras agencias fueron fundamentales cuando iniciaron las discusiones de las iniciativas de protección de datos en posesión de particulares. "En alguna ocasión en un evento público María Marván me preguntó si yo estaba a favor o en contra de que hubiese una autoridad o dos autoridades, una de transparencia y otra de protección de datos, que estuviesen separadas. Con base en mi experiencia, yo consideré que quizá era mejor dos autoridades. Luego me comentó María Marván: José Luis no sabes tú lo que nos ha influenciado aquella opinión tuya. Porque además dije *creo que quizá si hubiese una sola autoridad se pudiera generar una suerte de esquizofrenia,* y yo utilicé esa palabra. Pero es que José hasta en el Congreso, en el Senado nos han dicho que un experto internacional ha dicho que *eso puede generar una esquizofrenia*. Y le dije: María, pues no sabes cuánto lo siento, porque ahora he cambiado de opinión, después de haber ahondado mucho en el tema, creo que lo mejor sería que hubiese sólo un órgano. Y yo abogaba por que el IFAI fuese quien tuviese las funciones de protección de datos, y creo que esa es la mejor opción a la que se ha podido llegar" (José Luis Piñar, entrevista personal, 2 de octubre de 2014).

El apoyo internacional que tuvo el IFAI, su experiencia en la garantía de datos personales en posesión del sector público, el reconocimiento público, el impacto económico, el argumento sobre la unicidad de criterios en la interpretación de las leyes y el impulso propio del IFAI al ser el garante de la protección de datos personales desde 2003 —independientemente que sólo haya sido para el sector público—, además de la coincidencia de las características orgánicas

dentro de la administración pública que se solicitaban en su mayoría en las iniciativas de ley: ser un organismo público, descentralizado de la administración pública, con patrimonio propio, fueron los argumentos y los motivos para que el IFAI fuera el garante de la protección de datos en posesión de los particulares. La decisión de que el IFAI fuera la autoridad garante de la protección de datos no fue sencilla. El sector privado pugnaba por que se creara un organismo independiente del IFAI o fuera la Secretaría de Economía la autoridad garante.

De las ocho propuestas tres consideraban que el IFAI debería quedarse con la facultad de proteger los datos personales y los otros cinco que debería crearse una autoridad diferente al IFAI para ser garante de la protección de datos. Miguel Barbosa planteaba el Registro Nacional de Protección de Datos incorporado al INEGI; otros dos consideraban necesario un Instituto Federal de Protección de Datos Personales; otras dos proponían una Comisión Nacional de Protección de Datos Personales y una más un Instituto de Protección de Datos Personales. La Comisión Nacional de Protección de Datos Personales fue propuesta por Gustavo Parra y era la única que manifestaba la necesidad de que tuviera autonomía técnica, de gestión y en sus resoluciones. También proponía que fuera un organismo descentralizado de la administración pública centralizada, al igual que Adolfo Mota. La diferencia entre la propuesta de Parra y la de Mota fue que el último decía que el Instituto debería ser dependiente de la Secretaría de Economía. En este sentido ninguna propuesta consideraba que debería ser un órgano autónomo. Sí planteaban la independencia, incluso cierto tipo de autonomía —como la propuesta de Gustavo Parra—, pero no la autonomía constitucional.

3.2.3 Autoridad autónoma y nacional, INAI

La autonomía constitucional fue una necesidad posterior. Una vez publicadas las reformas y la Ley Federal de Protección de Datos Personales en posesión de los particulares se realizaron diversos estudios y propuestas legislativas (2011) para que el IFAI fuera una autoridad autónoma constitucional. Uno de los precedentes importantes fue “presentado por el Grupo Parlamentario del PRI en el Senado en la LXI Legislatura. El 13 de septiembre de 2011, los Senadores Manlio Fabio Beltrones y Raúl Mejía González, a nombre de todo el Grupo Parlamentario del PRI, presentaron una iniciativa para reformar los artículos 6° y 105 constitucionales. En esa iniciativa se argumentó que otorgar al IFAI un auténtico carácter de órgano de Estado era una condición necesaria para consolidar la democracia en torno al derecho de acceso a la información, así como el fortalecimiento de las funciones de la autoridad garante.

Posteriormente se presentó una iniciativa por parte del presidente Enrique Peña Nieto, el 10 de septiembre de 2012. Fue presentada a diputados del PRI y del Partido Verde Ecologista de México. Esta iniciativa propuso que el IFAI fuera constituido como el único organismo garante especializado, imparcial y autónomo en materia de los derechos de acceso a la información y protección de datos personales en posesión de cualquier autoridad, entidad, órgano u organismo federal. Su mandato abarcaba a todos los Poderes Federales y a los organismos con autonomía constitucional. A esta iniciativa se integraron otras más. Una presentada por la Senadora Laura Rojas Hernández (PAN); otra por el Senador Alejandro Encinas Rodríguez (PRD) y la última retomada por la Senadora Arely Gómez González (PRI y PVEM).

La autonomía del IFAI se reconoce oficialmente en el Diario Oficial de la Federación el viernes 7 de febrero de 2014. A partir de allí entra en vigor su autonomía constitucional y diversas funciones, atribuciones y competencias que se profundizan con las propuestas de leyes generales tanto de acceso a la información, como de protección de datos presentadas en octubre de 2014. Siendo, en 2016 aprobada la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados la norma que trató de crear un marco general estandarizado para la protección de este derecho en todo el territorio nacional y con alcance principalmente en el sector público.

Como se puede observar, el diseño de las normas, los valores, los principios y las reglas del juego (Douglas North, 1990) fue una negociación económica y política. Fue económica porque quienes modificaron e incluso detuvieron las iniciativas en el Congreso en materia de datos personales fueron las organizaciones empresariales, siendo los mecanismos del uso y tratamiento de datos parte de sus principales necesidades. Y fue una negociación política porque desde el mismo Congreso se favorecían temas, propuestas e iniciativas.

Hasta aquí, hemos identificado parte de los actores involucrados, sus intereses y la mayoría de los elementos formales, estructurales y constitucionales que favorecieron o limitaron este diseño tanto normativo, como de la autoridad garante, el IFAI —ahora INAI—. De una autoridad descentralizada de la administración pública pasó a ser una autoridad autónoma y recientemente nacional. Se ha encontrado que el diseño mexicano para la protección de datos personales se inclinó por una estructura mixta de regulación y organización. Este diseño le dio la posibilidad de incorporar a sectores diversos en la discusión para su puesta en agenda pública.

En el siguiente capítulo se analiza el caso del uso de datos personales en la *e.firma*, del Servicio de Administración Tributaria (SAT). Este caso nos permitirá observar de manera

cercana la aplicación de este diseño institucional y organizacional en un caso concreto, por los siguientes motivos: como se pudo observar el diseño institucional tiene una debilidad en el sector público, de allí la necesidad de una ley general, que estandarice reglas en todo el sector público. El análisis de este caso permitirá obtener elementos para concluir con mayor contundencia, mejoras para el diseño institucional y organizacional para la política de protección de datos personales en México. Otro de los motivos es porque la *e.firma* implica el tratamiento de datos biométricos, considerados como de alta sensibilidad en su uso y protección, y finalmente porque es un servicio que implica a los tres sectores definidos implicados en la regulación de este derecho, el sector público, el privado y a la persona en lo particular.

CAPÍTULO 4. El ANÁLISIS DEL USO DE DATOS PERSONALES EN LA FIRMA ELECTRÓNICA

El objetivo de este capítulo es analizar el diseño institucional y organizacional de la protección de datos personales en relación con el tratamiento de datos personales en la firma electrónica (*e.firma*) en el Servicio de Administración Tributaria (SAT). Este caso es relevante porque es una base de datos importante en México; es un servicio y un requerimiento de la administración pública para las personas físicas y morales; integra información biométrica de particulares considerada como de alto nivel de sensibilidad y protección en las legislaciones nacionales e internacionales, y finalmente porque en el tratamiento participa el sector público, el privado y la persona.[37]

Para estudiar el caso, se presentarán dos tipos de análisis que se fundan en el análisis e interpretación jurídica. El primero será de la norma nacional y el segundo el análisis basado en la interpretación sistemática e integral de las normas jurídicas aplicables al caso de algunos preceptos internacionales, este último análisis nuevos mecanismos de protección y con base en las últimas reglas aprobadas en la Comunidad Europea, el Reglamento Europeo de Protección de Datos Personales.

Antes de iniciar, primero se describen las generalidades del caso. Se explican las funciones del SAT, su relación con el Padrón de Contribuyentes (PC) y el Registro Federal de Contribuyentes (RFC); el objetivo de la *e.firma*, el fundamento jurídico; su relación con el SAT y la materia fiscal, todos temas necesarios para conocer el tratamiento administrativo de los datos personales. Una vez que se integra la explicación general del caso, se inicia con el análisis de éste. Como parte de la metodología se tuvo una entrevista con Fernando Martínez Coss, funcionario con más de 29 años de servicio en el SAT y se realizó un estudio profundo de investigación jurídica para lograr el estudio de caso.

4.1 La recolección de datos personales en los gobiernos

Desde la antigüedad, los gobiernos han tenido la necesidad de recopilar información de su población para sustentar en ella sus decisiones, servicios, obligaciones y derechos. Los registros

[37] Existen otros casos de suma importancia que podrían ser parte de investigaciones futuras. Tales como el expediente médico en el sector público, los datos personales en archivos históricos, los registros nacionales de población, entre otros, sin embargo para cada caso se requieren de investigaciones específicas, las cuales surgen como propuestas futuras a partir de esta investigación.

de población, propiedades y tributos son algunos ejemplos de ello. Así, en el año 3000 a.C., los Babilonios usaban pequeñas tablillas de arcilla para recopilar datos sobre la producción agrícola y los egipcios lo utilizaban para conocer los datos de su población y la riqueza de sus integrantes. Uno de los ejemplos más claros de la recolección de datos fue la utilización de censos en la Roma antigua. Éstos aparecen con las reformas de Servio Tulio, mismos que "le permitieron administrar tanto la guerra como la paz, así como las distintas obligaciones públicas de los ciudadanos" (Cañas, 2005: 456). Los censos permitían también "llevar a cabo la distribución de los ciudadanos en las distintas tribus y centurias, pudiendo modificar su situación en el censo anterior en función del poder que se atribuía a los censores (Fernández, 2013)[38], la nota contenía los siguientes datos:

- "Nombre y edad del ciudadano,
- Número de hijos,
- Bienes inmuebles sobre los que el censado tenía *dominium ex iure quiritum*[39],
- Esclavos de su propiedad,
- Armas de que disponía,
- Clientes que patrocinaba" (Cabañas, 2005: 459)

Como podemos observar, la información de las personas recabada en los censos podía ser utilizada por los gobiernos con diversos fines, incluso "se podía expulsar a un ciudadano y privarlo del voto. Es posible que la nota censoria se inscribiera junto al nombre del ciudadano. Otra sanción se presentaba cuando el encargado de realizar el censo era el cónsul, éste podía castigar por sí mismo, con penas sobre el cuerpo o sobre la vida, a aquellas personas que realizaban declaraciones falsas o no realizaran ningún tipo de declaración estando obligados a ello". El censo era por lo tanto una mezcla de información de la población, del catastro y del registro hipotecario" (Cabañas, 2005: 406), mediante el cual podían controlar los comportamientos sociales, políticos y militares de sus ciudadanos.

México tiene "más de cien años de historia censal. Se iniciaron de manera regular en 1895, y a partir de 1900 se realizan cada 10 años, con excepción de 1921. En 1950, se incorporó la temática de vivienda y en 1980 se agrega la de hogares" (Mantilla, 2008: 8).

[38] Dentro de las funciones de los censores se encontraba la *cura morum*, mediante la cual conservan las buenas costumbres. Para profundizar más sobre este tema se recomienda revisar: Baquero, María Eva (2013.) *The activity of the censors in the Administration of the roman Republic.* Disponible el 5 de octubre de 2016 en www.iustel.com/v2/revistas/detalle_revista.asp?id_noticia=412967.

[39] Dominio sobre la propiedad, protegido por el derecho de los primeros habitantes de Roma.

El censo no es la única base gubernamental que contiene datos personales, pero sí es una de las más completas en posesión gubernamental, vía el Instituto Nacional de Estadística y Geografía (INEGI). Los datos e información que se recopilan son de toda la población que habita el territorio nacional, independientemente de su calidad migratoria. En consecuencia, los censos y los conteos de población permiten conocer el cambio poblacional en un punto del tiempo según territorios específicos; las características de hogares y viviendas particulares y, por supuesto, las características individuales de las personas que habitan esas viviendas y hogares. En el siguiente cuadro se muestran algunos datos contenidos en los censos de población.

Cuadro 9. Datos contenidos en los censos.

Sobre las viviendas	Sobre las personas
• Tipo y clase de vivienda. • Condición de habitación. • Material predominante en paredes, pisos y techos. • Disponibilidad de cuarto para cocinar. • Número de dormitorios y de cuartos. • Servicios básicos: agua (dotación de agua), electricidad y drenaje. • Combustible usado para cocinar. • Eliminación y recolección de basura. • Tenencia. • Forma de construcción. • Antigüedad. • Equipamiento. • Bienes y servicios	• Nombre, • Sexo, edad, lugar de nacimiento. • Ascendencia y descendencia familiar. • Discapacidad (es). • Afiliación ideológica y religiosa. • Origen lingüístico (condición de habla indígena y española; y tipo de lengua indígena). • Movimientos migratorios (cinco años atrás). • Formación académica. • Nivel de escolaridad, alfabetismo, antecedente escolar y lugar de estudio. • Número de hijos nacidos vivos y fallecidos. • Lugar de residencia de los hijos sobrevivientes. • Situación conyugal. • Actividad (es) laboral (es). • Ingresos económicos. • Lugar de trabajo. • Adicciones. • Costumbres alimenticias • Condiciones de vivienda • Historia familiar • Nivel de ingresos

Fuente: Elaboración propia con datos de los cuestionarios del censo 2010.

Uno de los principios que rige el tratamiento de datos en el INEGI es la disociación de datos de las personas en lo particular. Es decir, se prevé que los datos no puedan identificar o hacer identificable a una persona en lo particular. En origen toda la información es anonimizada y con ello general y no específica sobre una persona, sino sobre la población o grupos poblacionales en lo general. Sin embargo, es importante reconocer que existe la posibilidad de vulneración y riesgo en el uso y tratamiento de los datos personales allí contenidos porque el cuestionario pide datos personales

de los habitantes de vivienda, incluyendo nombre, edad, sexo y otros datos de mayor sensibilidad (INEGI, 2010).

La información generada por los censos es un instrumento fundamental para proveer al país de la información necesaria "para planear y fundamentar sus decisiones para el desarrollo de políticas públicas, programas de gobierno, estrategias e inversiones económicas o científicas" (INEGI, 2012) e incluso para la evaluación de esos programas o decisiones. Esta información no sólo es utilizada por el gobierno sino también por las empresas, asociaciones e investigadores y en general todos pueden acceder a la información generada por los censos de población.

Otra "base de datos nacional" (Garfinkel, 2000) en México es el Padrón de Electores con 84,686, 713 (INE, 2016) registros que la Dirección Ejecutiva del Registro Federal de Electores del Instituto Nacional Electoral se encarga de recopilar, administrar y resguardar. La información que contiene es: nombre, dirección particular, edad, año y lugar de nacimiento, clave de elector, Clave Única del Registro de Población (CURP), firma, fotografía y registro dactilar (huellas digitales). Esta información es proporcionada, en su totalidad, a representantes de partidos políticos acreditados ante el Instituto en sus diferentes sedes nacionales, locales o regionales; asimismo, se distribuye a los diferentes consejos nacionales, locales y distritales.

Tenemos también el Registro Nacional de Población (RENAPO), al que nos referiremos más adelante por ser parte del objeto de estudio de este caso. Además de los anteriores, entre otros registros gubernamentales, podemos encontrar el Registro Federal de Contribuyentes (RFC), las bases de datos de los registros civiles y de la propiedad y del comercio de las entidades federativas, la Clave Única de Registro de Población, el Registro Público Vehicular y el Registro Nacional de Profesiones (RNP), así como los respectivos registros en posesión de universidades públicas y privadas.[40]

En torno a estas bases de datos nacionales, también se encuentra el RFC como una de las bases de datos más importantes. Tanto por la función que cumple como por los datos que contiene, especialmente en lo concerniente a la Firma Electrónica (*e.firma*) que incorpora datos biométricos considerados como sensibles y cuyo registro realiza y administra el Sistema de Administración Tributaria (SAT), información que será analizada en el siguiente apartado,

[40] En un sector que genera incertidumbre sobre su situación y definición jurídica hay datos en posesión de los partidos políticos: principalmente padrón de afiliados. En este mismo rubro también se ubican los sindicatos y las asociaciones civiles o fundaciones, denominadas como instituciones sin fines de lucro o instituciones de interés común. Finalmente, es indispensable considerar los archivos en posesión de la(s) iglesia (s) vía los registros que prestan a sus feligreses por servicios religiosos

específicamente en cuanto al hecho de que los contribuyentes sean obligados a proporcionar sus datos biométricos para obtención de la firma mencionada.

4.2 El Servicio de Administración Tributaria (SAT)

El SAT surge en julio de 1997, aunque la ley que le dio origen fue aprobada en 1995 (Velazco, 2008: 15), y se crea como "un órgano desconcentrado de la Secretaría de Hacienda y Crédito Público, con carácter de autoridad fiscal con atribuciones y facultades vinculadas con la determinación y recaudación de las contribuciones federales que tenía a su cargo la Subsecretaría de Ingresos". Surge como una necesidad institucional por la propia dinámica económica y social del país. El modelo estuvo influenciado por el sistema de Nueva Zelanda, Australia y especialmente el de España" (entrevista con Fernando Martínez, 19 de agosto de 2016).

El SAT tiene como régimen normativo diversos ordenamientos tales como el Código Fiscal de la Federación y su Reglamento, leyes, otros reglamentos, lineamientos, acuerdos, decretos, entre otras normas. Por ejemplo, en la Constitución Política de los Estados Unidos Mexicanos (CPEUM) en el artículo 31, fracción IV, se establece la obligatoriedad de los ciudadanos para aportar al gasto público mediante las contribuciones. De ahí se deriva el artículo 27 del Código Fiscal de la Federación, que dice "Las personas morales, así como las personas físicas que deban presentar declaraciones periódicas o que estén obligadas a expedir comprobantes fiscales digitales por Internet por los actos o actividades que realicen o por los ingresos que perciban, o que hayan abierto una cuenta a su nombre en las entidades del sistema financiero o en las sociedades cooperativas de ahorro y préstamo, en las que reciban depósitos o realicen operaciones susceptibles de ser sujetas de contribuciones, deberán solicitar su inscripción en el registro federal de contribuyentes, proporcionar la información relacionada con su identidad, su domicilio y, en general, sobre su situación fiscal" (Art. 27, CFF).

Asimismo, dentro de las diversas facultades que tiene el SAT se encuentran tres de trascendencia: aplicar la legislación fiscal y aduanera; fiscalizar a los contribuyentes para verificar que cumplan con esta legislación y promover que los contribuyentes cumplan voluntariamente con sus obligaciones (Velazco, 2008: 15). Es decir, tiene la facultad para determinar, liquidar y recaudar las contribuciones para el financiamiento del gasto público.

La definición más amplia de las facultades de la autoridad fiscal está en el Código Fiscal Federal, que las agrupa de esta forma:

a) Asistencia al contribuyente, para ayudarlo a cumplir voluntariamente con sus obligaciones, proporcionarle toda la información necesaria y facilitarle los trámites.
b) Comprobación, que implica realizar las auditorías y revisiones necesarias para verificar que los contribuyentes efectivamente cumplan con sus obligaciones;
c) "Determinar las contribuciones o aprovechamientos omitidos y sus accesorios, así como imponer sanciones por infracciones a las disposiciones fiscales.
d) Investigar hechos constitutivos de delitos en materia fiscal" (Velazco, 2008: 16).

El SAT, para cumplir con sus obligaciones y prestar su servicio, se fundamenta en el Padrón de Contribuyentes, el cual se integra por los datos de las personas que se han inscrito, a efecto de cumplir con sus obligaciones fiscales y las aportaciones al gasto público. En el siguiente apartado se profundiza sobre su estructura y función.

4.3 El padrón de contribuyentes

De las grandes bases de datos nacionales que posee el gobierno en México se encuentra el padrón de contribuyentes, con un total de 71, 795, 905 registros (SAT, 2019), de los cuales se pueden clasificar en personas físicas, asalariados y personas morales.

Cuadro 10. Tipología de contribuyentes

Año	Mes	Personas Físicas	Asalariados (PF)	Personas Morales	Total
2015	Diciembre	19.942.949	29.855.002	1.763.655	51.582.845
2016	Diciembre	22.222.004	32.702.983	1.843.027	56.794.640
2017	Diciembre	24.780.762	37.926.366	1.932.287	64.672.335
2018	Diciembre	28.198.662	41.510.280	2.043.880	71.795.905

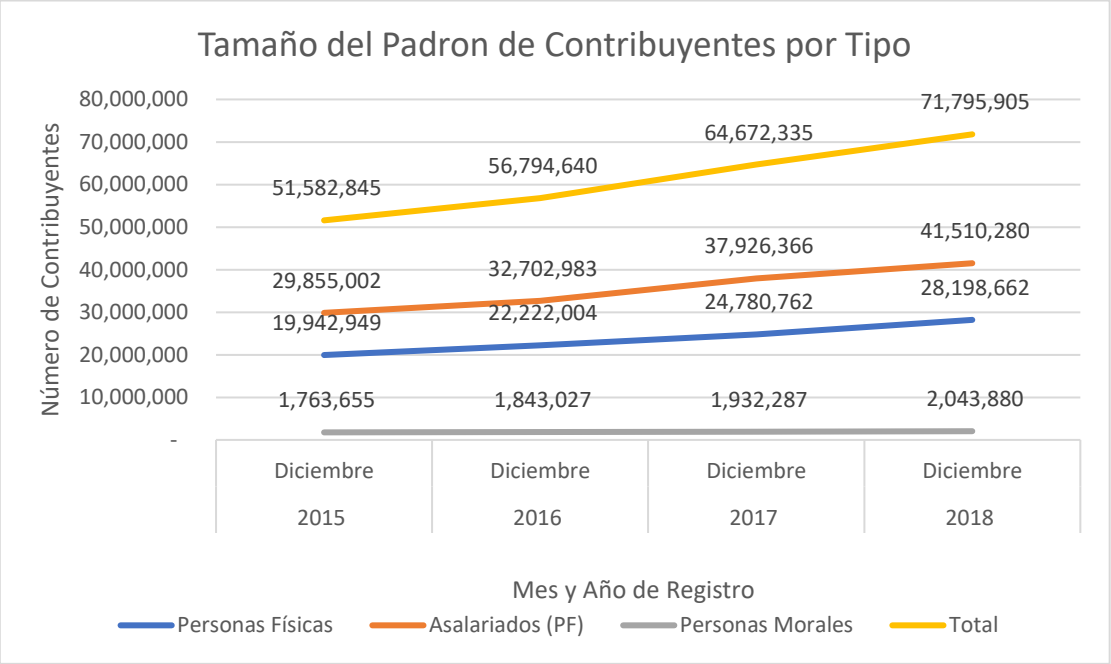
Fuente: SAT, 2019. *Datos abiertos*. Disponible en: http://omawww.sat.gob.mx/cifras_sat/Paginas/datos/vinculo.html?page =giipTipCon.html

Tal como se puede ver en el cuadro anterior, el SAT tiene una tipología de contribuyentes: personas físicas, asalariados, personas morales y tanto personas físicas o morales los subclasifica por tamaño. Los registros que integran el padrón de contribuyentes cuentan con datos personales,

entre los cuales están los datos biométricos, así como las huellas dactilares y la imagen del iris, datos considerados como sensibles y de máxima protección. Esta es otra característica de este padrón que nos permite elegirlo como un caso de estudio. Es importante señalar que no todos los adscritos al padrón de contribuyentes se les solicita la misma información.

Gráficamente la información sobre el número de contribuyentes del SAT, según su tipo, se observa de la siguiente manera.

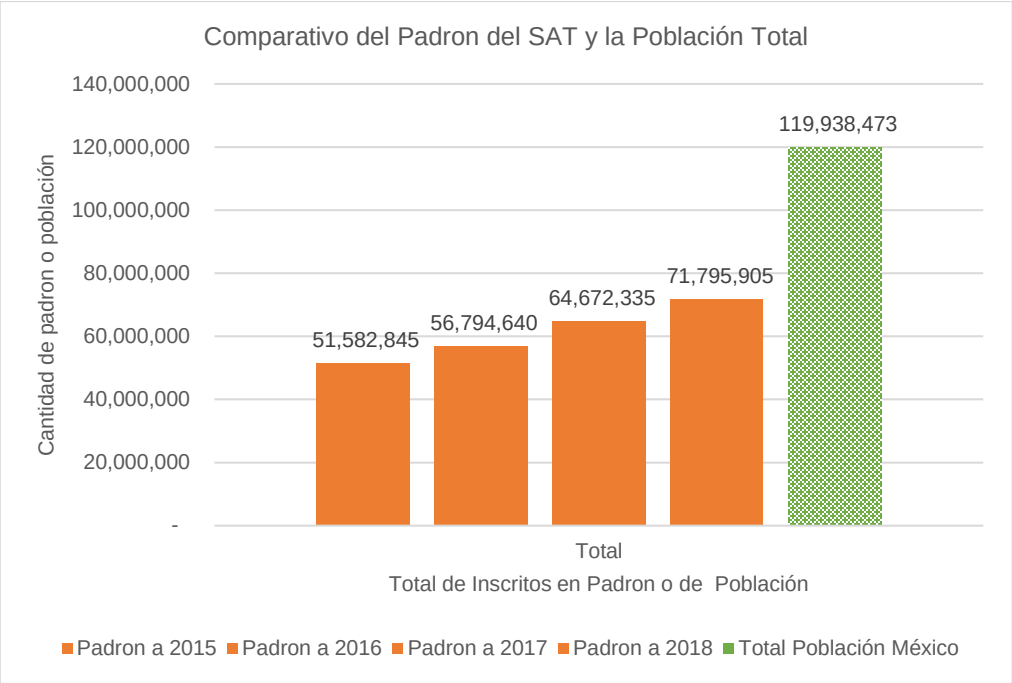
Gráfica 1. Padrón de contribuyentes por tipo



Fuente: Elaboración propia con datos de SAT, 2019. *Datos abiertos*. Disponible en: http://omawww.sat.gob.mx/cifras_sat/Paginas/datos/vinculo.html?page=giipTipCon.html

En la gráfica se muestra que el total de personas con régimen de asalariados son superiores a los otros regímenes. Le sigue el régimen de personas físicas, y posteriormente el de personas morales. Ahora bien, si realizamos un comparativo entre el total de la población y el número del padrón de contribuyentes obtendremos los resultados siguientes:

Esquema 11. Población vs. contribuyentes



Fuente: elaboración propia con datos de SAT e INEGI, 2019.

Este comparativo nos permite identificar la importancia de esta base de datos y su trascendencia en el entorno gubernamental. Como mencionamos anteriormente, el padrón de contribuyentes, que contiene los RFC y otros datos, es una de las bases de datos más grandes en México, pertenece al ámbito gubernamental y se relaciona con otros actores públicos y privados; es utilizada para diversos trámites y para cumplir diversas obligaciones con el Estado (la declaración de impuestos y el cumplimento de acreditar la identidad fiscal). Es, además, un medio de identificación económica, financiera nacional e internacional, porque con la *e.firma* se pueden hacer transacciones comerciales y aduaneras.

El padrón de Contribuyente se integra principalmente por el RFC, mismo que es un dato personal constituido por diversos datos personales. El INAI así lo define:

> "El Registro Federal de Contribuyentes (RFC) de las personas físicas es un dato personal confidencial. De conformidad con lo establecido en el artículo 18, fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental se considera información confidencial los datos personales que requieren el consentimiento de los individuos para su difusión, distribución o comercialización en los términos de esta Ley. Por su parte, según dispone el artículo 3, fracción II de la Ley Federal de Transparencia

> y Acceso a la Información Pública Gubernamental, dato personal es toda aquella información concerniente a una persona física identificada o identificable. Para obtener el RFC es necesario acreditar previamente mediante documentos oficiales (pasaporte, acta de nacimiento, etc.) la identidad de la persona, su fecha y lugar de nacimiento, entre otros. De acuerdo con la legislación tributaria, las personas físicas tramitan su inscripción en el Registro Federal de Contribuyentes con el único propósito de realizar mediante esa clave de identificación, operaciones o actividades de naturaleza tributaria. En este sentido, el artículo 79 del Código Fiscal de la Federación prevé que la utilización de una clave de registro no asignada por la autoridad constituye como una infracción en materia fiscal. De acuerdo con lo antes apuntado, el RFC vinculado al nombre de su titular, permite identificar la edad de la persona, así como su homoclave, siendo esta última única e irrepetible, por lo que es posible concluir que el RFC constituye un dato personal y, por tanto, información confidencial, de conformidad con los previsto en el artículo 18, fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (INAI, 2009).

Ante esta resolución del INAI, es importante analizar de manera específica la *e.firma*. Para obtenerla, según el párrafo quinto del artículo 17-D del Código Fiscal de la Federación, debe ser tramitada por los contribuyentes ante el Servicio de Administración Tributaria o cualquier prestador de servicios de certificación autorizado por el Banco de México, firma que es el objetivo específico de estudio de este apartado, ya que además de incluir al RFC, incorpora información que permite identificarte, incluso con información confidencial sensible, considerada como de máxima protección, como lo son los datos biométricos: ocho huellas digitales, el reconocimiento facial y el iris ocular.

4.4 La firma electrónica (*e.firma*)

La firma electrónica, según el artículo 2, fracción XIII, de la Ley de Firma Electrónica Avanzada, es “el conjunto de datos y caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa.”

Durante el proceso para la obtención de la *e.firma*, el SAT recaba datos biométricos, con

la finalidad de garantizar el vínculo entre el certificado y su titular (SAT, 2016).[41] El procedimiento para la obtención de la *e.firma* es el siguiente:

1. Se acude a cualquier oficina del SAT de forma física.
2. Es personalísima para el caso de las personas físicas.
3. Puede ser por representación (poder), legal notariada y/o certificada para personas morales.

Para personas físicas:

1. Presentar original o copia certificada de una identificación oficial vigente.
2. Presentar CURP y verificar si la CURP está certificada en el Registro Nacional de Población; en caso contrario, se debe presentar acta de nacimiento en original.
3. Original del comprobante de domicilio fiscal, únicamente para contribuyentes que se hayan inscrito al RFC con CURP, por Internet. En el caso de asalariados, también se acepta la credencial para votar expedida por el Instituto Nacional Electoral (antes Instituto Federal Electoral) para acreditar el domicilio (siempre y cuando en ésta se señale el mismo).

Además, para personas morales:

4. En caso de personas morales, el representante legal debe contar con Firma Electrónica Avanzada (activa) y presentar el poder general para actos de dominio o de administración, así como el acta constitutiva en original o copia certificada ante Notario Público.

Como requisito indispensable para tener la *e.firma* se debe obtener el archivo con extensión *.req y la llave privada.* Son dos procesos que se deben realizar anteriormente. Al concluir el trámite se otorga el archivo digital con la *e.firma* y las contraseñas necesarias para ser utilizada. Los datos que se recolectan son los siguientes:

- Nombre completo
- Fecha de nacimiento
- Lugar de nacimiento
- Domicilio

[41] SAT (2016). Preguntas Operativas.

- Domicilio fiscal
- Correo electrónico (que será público)
- Edad
- 10 imágenes de huellas digitales
- Firma autógrafa
- Imagen facial
- Iris de ambos ojos

Con esta información, además, se puede acceder a la siguiente información personal:

- Percepciones económicas
- Lugar (es) laboral (es),
- Relaciones laborales
- Situación financiera
- Obligaciones fiscales
- Situación fiscal

De acuerdo con la entrevista realizada a Fernando Martínez Coss (19 de agosto de 2016), quien era Administrador Central de Gestión de Servicios y Trámites con Medios Electrónicos del Servicio de Administración Tributaria, el objetivo de la *e.firma* es "identificar y asegurar la identidad del emisor de un mensaje y/o relación económica financiera, como autor legítimo de éste, tal y como si se tratara de una firma". Además de ser útil al momento de realizar las declaraciones anuales de impuestos, la *e.firma* también es utilizada para:

- Pedimentos por parte de los agentes aduanales.
- Dictámenes fiscales
- Para consultar los expedientes fiscales de forma electrónica en la página del SAT.
- Para emitir comprobantes fiscales digitales.
- Para solicitar devoluciones cuyo importe sea mayor o igual a los 10,000 pesos. (*Expansión*, 2011).

Todos los documentos que "se proporcionan al SAT son cotejados con dos entidades: la Secretaría de Gobernación (SG) para el caso de la información de identidad, como la CURP. Y para el caso de la información para la creación de los certificados digitales el cotejo es con el Banco de México. La base de datos, "las concentra el SAT y es una empresa privada quien es la

encargada de proveer las herramientas tecnológicas" (entrevista personal a Fernando Martínez Coss, 19 de agosto de 2016).

Los "mecanismos de seguridad son a través de los protocolos del Banco de México" y todas las herramientas tecnológicas y el servicio de acreditación de identidad y enrolamiento lo realiza una empresa privada. Del 26 de marzo de 2015 al 25 de marzo de 2019 se ha cedido el contrato a *Acerta Computaciones Aplicadas S. A. de C. V,* quien será la encargada de "asegurar la continuidad del servicio de acreditación de identidad y enrolamiento de contribuyentes para la Firma Electrónica, a través de herramientas tecnológicas seguras y confiables, implementando las mejoras de acuerdo a la evolución operativa y tecnológica." Según lo menciona el contrato de licitación para la empresa (SAT, 2016).[42]

Para el manejo de la información en el SAT, según Fernando Martínez Coss (entrevista personal a Fernando Martínez Coss, 19 de agosto de 2016) la identidad es la piedra angular en las transacciones en internet, motivo por el cual los documentos probatorios de identidad presentados por el contribuyente se cotejan contra la base de datos del SAT, como los datos Biométricos. Si no existe diferencia entre los documentos probatorios de identidad y la base de datos, se registran los datos personales de los contribuyentes y se da continuidad a los trámites solicitados. Por ejemplo, cuando se registran, el cotejo con la SG se realiza para verificar que la CURP sea auténtica y se encuentre en la base de datos de la SG. Para junio de 2015 se tenía un registro de la identidad única digital de 6.4 millones de contribuyentes. Dentro de los cuales se encontraban los siguientes datos:

Imagen 1. Datos para obtener la *e.firma*

Fuente: SAT, 2015.[43]

[42] Para conocer más acerca de los proyectos contratados sobre información y seguridad de la información en 2016 el Servicio de Administración tributario, recomiendo consultar el portafolio de proyectos contratados a 2016.

[43] SHCP y SAT. 2016. Uso de documentos digitales para facilitar y simplificar el cumplimiento fiscal. Documento realizado en agosto 2015. Consultado el 17 de agosto de 2016. Disponible en: http://www.ateb.mx/wp-content/uploads/2015/08/Uso-de-documentos-digitales.pdf

Después de un año, la base de datos personales aumentó en poco más de un millón, tan es así que, para el mes de junio de 2016, se contaba con 7 millones 608 mil contribuyentes realizando el trámite de la *e.firma*. Esto generó la expedición de 13.2 millones de certificados de firmas electrónicas (SAT, 2016). Las estadísticas de 2011 a 2016 son las siguientes:

Cuadro 11. Firma Electrónica. Datos acumulados.

Año	Contribuyente que han tramitado la Firma Electrónica (*e.firma*)
2013	6,587,812
2014	7, 912,029
2015	8,970,992
2016	10,250,907
2017	11,784,940
2018	12,602,008

Fuente: SAT, 2019.[44]

Entonces son aproximadamente 12 millones y medio de contribuyentes que cuentan con *e.firma*. En el siguiente apartado se estudia quiénes están obligados a realizar el registro.

4.5 Obligatoriedad del registro

En México, el artículo 31 de la Constitución Política de los Estados Unidos Mexicanos, dice que una de las obligaciones de los mexicanos es "contribuir para los gastos públicos, así de la Federación, como de los Estados, de la Ciudad de México y del Municipio en que residan, de la manera proporcional y equitativa que dispongan las leyes" (CPEUM, Artículo 31, fracción IV, 2019).

Para cumplir con sus obligaciones los contribuyentes, según el artículo 27 del Código Fiscal de la Federación dice que:

> "Las personas morales, así como las personas físicas que deban presentar declaraciones periódicas o que estén obligadas a expedir comprobantes fiscales digitales por internet por los actos o actividades que realicen o por los ingresos que perciban, o que hayan abierto una cuenta a su nombre en las entidades del sistema financiero o en las sociedades

[44] Informe tributario y de gestión. Junio de 2019. Consultado el 20 de marzo de 2019 en: http://omawww.sat.gob.mx/transparencia/Documents/ITG%202do%20trimestre%202018_180828.pdf

> cooperativas de ahorro y préstamo, en las que reciban depósitos o realicen operaciones susceptibles de ser sujetas de contribuciones, *deberán solicitar su inscripción en el registro federal de contribuyentes*, proporcionar la información relacionada con su identidad, su domicilio y, en general, sobre su situación fiscal, mediante los avisos que se establecen en el reglamento de este código" (CFF, Art, 27, 2016)
>
> […] Las personas morales y las personas físicas que deban presentar declaraciones periódicas o que estén obligadas a expedir comprobantes fiscales por los actos o actividades que realicen o por los ingresos que perciban, *deberán solicitar su certificado de firma electrónica avanzada* […]

La autoridad encargada de llevar el registro es el SAT y se basa en la información que proporcionan los contribuyentes, además de hacerla verificable por medios como los proporcionados por la Secretaría de Gobernación. El SAT a su vez asigna una clave a cada persona inscrita, la cual también es un dato personal, tal como lo confirmado en el INAI.

Aun cuando hay muchas otras especificidades sobre las funciones del SAT, hemos abordado las generalidades de la base de datos tanto del RFC como de la *e.firma*. A continuación, se realiza un análisis normativo y de principios de protección de datos personales enmarcados en el Convenio 108 de APEC, la Directiva 95, Resolución de Madrid y el Marco de Privacidad de APEC y así como en los lineamientos establecidos para la protección de datos que deberán observar las dependencias y entidades de la Administración Pública Federal.

Para finalizar, se propondrán procesos y procedimientos de mejora en el uso y manejo de datos personales para el sector público y privado, con base en el nuevo reglamento europeo de protección de datos personales, y las disposiciones administrativas y jurídicas que pudieran enriquecer el sistema de protección de datos personales en México, específicamente en el sector público a partir de la Ley General en la materia y el reciente Programa Nacional de Protección de Datos Personales 2018-2022.

4.6 Análisis normativo

Sobre el análisis normativo, incluye la interpretación de las normas. Rolando Tamayo y Salmorán (2003: 134-135), en su libro sobre razonamiento e interpretación jurídica, dice que la palabra interpretación alude a la intermediación para hacer entendible algo no claro. Por lo tanto, interpretar:

> “consiste en dotar de significado, mediante un lenguaje significativo, ciertas cosas, signos, fórmulas o acontecimientos (objeto significado). De allí que interpretar consista en un acto de significación, esto es, un acto por el cual se asigna un significado específico a ciertos hechos, signos, formulas o palabras. El acto de significación es simplemente expreso en un lenguaje” (Tamayo y Salmorán, 2003: 136)
>
> En este sentido, “la función significativa de la interpretación consiste en la incorporación de un determinado significado a ciertos signos, términos o palabras a fin de hacerlos corresponder con los determinados objetos”. El lenguaje interpretado puede ser simbólico, ideológico, algorítmico o idiomática; verbal o escrito. Es decir, no solo se refiere a establecer o declarar el significado de un texto (Tamayo y Salmorán, 2003: 138).

Entonces lo que aquí se pretende realizar es dotar de sentido y significado a la norma y al discurso institucional establecido con base en la teoría que sustenta esta investigación y los parámetros utilizados en el apartado teórico. No sólo se trata de un análisis de interpretación jurídica, sino que va más allá con la interpretación de los principios y el actuar ético tanto del Estado como de los ciudadanos.

Existen diferentes tipos de interpretación. Jacobo Pérez Escobar (1989) dice que existen los siguientes tipos: la interpretación jurisdiccional, la auténtica, la judicial, la doctrinal, la popular y la administrativa. “la interpretación popular es la interpretación que hacen todas las personas que no tienen formación jurídica; la doctrinal es la interpretación realizada por los expertos de la ciencia jurídica; la interpretación auténtica la realiza el legislador en el texto de la ley. Es denominada así, porque procede de su autor, conocer fielmente de su espíritu y de lo que propone; la administrativa es la interpretación que realiza el Ejecutivo por conducto de sus autoridades; la judicial es la interpretación que emana de los jueces y tribunales al realizar sus sentencias y resoluciones, y la jurisprudencial es la interpretación que emiten los máximos tribunales de la Nación y que se expresa en un criterio uniforme reiterado de interpretación.”

El primer análisis que se realiza es el normativo. El segundo será a partir de los principios de la protección de datos personales de los acuerdos internacionales de los que México es parte. Finalmente, estos análisis se amplían con el estudio de aspectos sociológicos, políticos y administrativos, tanto desde la teoría de las instituciones como de las organizaciones, dirigiendo el análisis a partir de los principios de protección de datos personales. Esto nos lleva incluso a discutir aspectos de derechos humanos, facultad de las instituciones gubernamentales y los retos que el tema plantea tanto para el sector público como el privado. Por lo tanto, los medios de

interpretación son variados y tratan de incorporar analíticamente riqueza al análisis e interpretación del caso.

Por lo tanto, este análisis se fundamenta en la Constitución Política de los Estados Unidos Mexicanos (CPEUM), la Ley Orgánica de la Administración Pública Federal (LOAPF), el Código Fiscal de la Federación (CFF), la Ley de la Firma Electrónica Avanzada (LFEA), la Ley General de Población (LGP), entre otros ordenamientos y algunas jurisprudencias que permitan identificar áreas de oportunidad en el tratamientos de datos personales y opciones para dotar de contenido la política de protección de datos personales en México.

4.6.1 El uso de datos personales en la *e.firma*

La Firma Electrónica (*e.firma*) es el conjunto de datos y caracteres que permite la identificación de una persona, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo firmante y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa (Art. 3, fracción XII, de la Ley de Firma Electrónica Avanzada).

Los datos a los que hace referencia la Ley son definidos por la propia Ley General de Población y las disposiciones de la Ley que regula la *e.firma* (Artículo 3, Fracción VIII). Al respecto, los artículos 85 y 86 de la LGP "establecen que la Secretaría de Gobernación tiene a su cargo el registro y la acreditación de la identidad de todas las personas residentes en el país y de los nacionales que residan en el extranjero, a través del Registro Nacional de Población (RENAPO) el cual tiene como finalidad registrar a cada una de las personas que integran la población del país, con los datos que permitan certificar y acreditar fehacientemente su identidad".

En ese registro "se inscribirá a los mexicanos, mediante el Registro Nacional de Ciudadanos y el Registro de Menores de Edad; y a los extranjeros, a través del Catálogo de los Extranjeros residentes en la República Mexicana" (artículo 87, fracciones I y II, respectivamente, de la LGP). Al respecto, el artículo 47 del reglamento de la LGP establece que el RENAPO se conforma con los datos de los mexicanos y mexicanas de dieciocho o más años, los cuales deberán ser, cuando menos, los siguientes:

a) Nombre completo.
b) Sexo del ciudadano.
c) Lugar y fecha de nacimiento.

d) Lugar y fecha en que se llevó a cabo la inscripción de la persona al Registro Nacional de Ciudadanos.
e) Nombre completo y nacionalidad del padre y la madre cuando se consignen en los documentos presentados.
f) Datos de localización del acta de nacimiento en el Registro Civil, o del certificado de nacionalidad, o de la carta de naturalización.
g) Nacionalidad de origen cuando el ciudadano haya adquirido la nacionalidad por naturalización.
h) Clave Única del Registro de Población, y

i) Fotografía, huellas dactilares, imagen del iris y firma del ciudadano.

Cabe mencionar que al incorporar a una persona en el RENAPO se le asigna una clave que se denomina Clave Única de Registro de Población (CURP), la cual servirá para registrarla e identificarla de forma individual (Artículo 91 de la LGP).

Por último, debe recalcar que de acuerdo con la LGP la Secretaría de Gobernación establecerá las normas, métodos y procedimientos técnicos del RENAPO. Asimismo, *coordinará los métodos de identificación y registro de las dependencias de la administración pública federal* (énfasis en cursivas añadido. Artículo 92).

4.6.2 Sujetos a disposición de la ley y ámbitos de competencia

Están sujetos a las disposiciones de la LFEA (artículos 2, fracción, y 3, fracciones II y III):

I. Las dependencias y entidades.
II. *Los servidores públicos* de las dependencias y entidades que en la realización de los actos a que se refiere esta ley utilicen la firma electrónica avanzada, y
III. *Los particulares*, en los casos en que utilicen la firma electrónica avanzada en términos de esta Ley.

Cabe resaltar que las disposiciones de la Ley que regula la *e.firma* no serán aplicables a:

I. Los actos en que no sea factible el uso de la firma electrónica avanzada por disposición de ley.
II. Aquéllos en que exista previo dictamen de la Secretaría; ni
III. **Las materias fiscal**, aduanera y financiera (Artículo 4).

Respecto de la excepción resaltada con negritas, parecería una contradicción lo dispuesto en el

segundo párrafo del Artículo 5 de la Ley que regula la *e.firma*, que a la letra dice:

> "La Secretaría, en el ámbito de su competencia, estará facultada para interpretar las disposiciones de esta Ley para efectos administrativos. La Secretaría, la Secretaría de Economía y el Servicio de Administración Tributaria dictarán, de manera conjunta, las disposiciones generales para el adecuado cumplimiento de esta Ley, mismas que deberán publicarse en el Diario Oficial de la Federación." (Artículo 5.)

Con el objetivo de aclarar dicha disposición, a través de una interpretación genérica de la norma, es importante considerar la "exposición de motivos"[45] en la que se argumenta y justifica que se "excluyen expresamente de la aplicación de esta Ley, los actos relacionados con las materias fiscal y aduanera, *en virtud de que tienen como objetivo proveer al Estado de los recursos necesarios para su funcionamiento,* […] "no obstante lo anterior, la iniciativa reconoce la importancia de la participación del SAT, como autoridad certificadora, para la expedición de certificados digitales en términos de la multicitada ley" (Cámara de Diputados, 2011: 12).

Como se puede observar, las disposiciones son ambiguas, toda vez que en la exposición de motivos se cita que la *e.firma* no se aplica en materia fiscal porque esta materia "provee de recursos necesarios para el funcionamiento del Estado". En este sentido, si se aplica la Ley se limitarían las transacciones a un mecanismo tecnológico que no permitiría la funcionalidad, eficiencia y continuidad de las funciones del Estado, deduciéndose de ello que el uso de la firma limitaría la provisión de recursos del Estado.

Lo anterior, considerando el ámbito de competencia del SAT, mismo que se establece en los artículos 1º y 2º de la Ley del Servicio de Administración Tributaria:

> "Artículo 1o. El Servicio de Administración Tributaria es un órgano desconcentrado de la Secretaría de Hacienda y Crédito Público, con el carácter de *autoridad fiscal*, y con las atribuciones y facultades ejecutivas que señala esta Ley.
>
> "Artículo 2o. El Servicio de Administración Tributaria tiene la responsabilidad de *aplicar la legislación fiscal* y aduanera con el fin de que las personas físicas y morales contribuyan proporcional y equitativamente al gasto público, de fiscalizar a los contribuyentes para que cumplan con las disposiciones tributarias y aduaneras, de facilitar e incentivar el cumplimiento voluntario de dichas disposiciones, y de generar y

[45] Senado de la República. 2010. Iniciativa del Ejecutivo que propone la creación de la Ley de Firma Electrónica Avanzada, presentada ante el Senado de la República el 9 de diciembre del 2010. Disponible en: http://www.senado.gob.mx/index.php?ver=sp&mn=2&sm=2&id=6754&lg=61

proporcionar la información necesaria para el diseño y la evaluación de la política tributaria."

Por su parte, el artículo 31 de la LOAPF establece que a la Secretaría de Hacienda y Crédito Público corresponde el despacho de los siguientes asuntos: XXII. Emitir políticas, normas, lineamientos y procedimientos en materia de adquisiciones, arrendamientos, servicios y obras públicas y servicios relacionados con las mismas de la Administración Pública Federal; emitir y en su caso opinar sobre las normas relacionadas con la desincorporación de activos; administrar el sistema COMPRANET, llevar los procedimientos de conciliación en dichas materias, en términos de las disposiciones respectivas y *aplicar la Ley de Firma Electrónica Avanzada.*

Como se puede observar, la materia fiscal va más allá de la tributación. Fernando Martínez Coss (entrevista, el 19 de agosto del 2016) dice que "para efectos de la ley de procedimientos administrativos los trámites tributarios no entran en todo el esquema de regulación, debido a esto se exentó del uso de la firma. Adicionalmente el SAT no solamente emite certificados de firma para personas físicas, objeto principal de la ley, también se emiten certificados para personas morales". Por lo tanto, es una contradicción. Si bien el uso obligatorio de la firma en materia fiscal sería más bien una traba a principalmente la provisión de recursos, la pregunta es ¿por qué es exigible para las personas físicas que requieren realizar transacciones fiscales con menor valor que las personas morales?

Entonces, se limita el uso de la *e.firma* en materia fiscal para liberar la recaudación de recursos del Estado; sin embargo, es exigible para las personas físicas. Esta disposición sólo es entendible cuando ampliamos el análisis, pues de otra manera sólo se puede decir que el uso de la firma no tiene fundamento legal en materia fiscal. De esta manera se carece de diseños institucionales y organizacionales sólidos y claros. Esta información es sumamente especializada y en general los ciudadanos la desconocen.

Es importante continuar con los aspectos de los datos personales que recolecta el SAT y que bien puede ser el RFC o los contenidos en la *e.firma*. Esta recolección de datos dice Fernando Martínez Coss, tiene su sustento tanto en lo que dice el CFF como la Ley General de Población. Al respecto, como hemos citado anteriormente, el artículo 17-D del Código Fiscal de la Federación señala que:

"cuando las disposiciones fiscales obliguen a presentar documentos, estos deberán ser

digitales y contener una firma electrónica avanzada del autor, salvo los casos que establezcan una regla diferente. Las autoridades fiscales, mediante reglas de carácter general, podrán autorizar el uso de otras firmas electrónicas."

La presentación de documentos digitales tiene un procedimiento establecido que consta de:

> "la creación de certificados que confirmen el vínculo entre un firmante y los datos de creación de una firma electrónica avanzada, expedido por el Servicio de Administración Tributaria cuando se trate de personas morales y de los sellos digitales previstos en el artículo 29 de este Código, y por un prestador de servicios de certificación autorizado por el Banco de México cuando se trate de personas físicas" (Artículo 17-D, CFF, 2016).

Los prestadores de servicios de certificación deberán ser publicados, avalados y autorizados por el Banco de México, y se realizará por medio del Diario Oficial de la Federación. Al respecto, como ya habíamos citado, "Los datos de creación de firmas electrónicas avanzadas podrán ser tramitados por los contribuyentes ante el Servicio de Administración Tributaria o cualquier prestador de servicios de certificación autorizado por el Banco de México" (Artículo 17-D, CFF, 2016). Asimismo:

> "Cuando los datos de creación de firmas electrónicas avanzadas se tramiten ante un prestador de servicios de certificación diverso al Servicio de Administración Tributaria, se requerirá que el interesado previamente comparezca personalmente ante el Servicio de Administración Tributaria para acreditar su identidad. En ningún caso los prestadores de servicios de certificación autorizados por el Banco de México podrán emitir un certificado sin que previamente cuenten con la comunicación del Servicio de Administración Tributaria de haber acreditado al interesado, de conformidad con las reglas de carácter general que al efecto expida. A su vez, el prestador de servicios deberá informar al Servicio de Administración Tributaria el código de identificación único del certificado asignado al interesado.
>
> La comparecencia de las personas físicas a que se refiere el párrafo anterior no podrá efectuarse mediante apoderado o representante legal, salvo en los casos establecidos a través de reglas de carácter general. Únicamente para los efectos de tramitar la firma electrónica avanzada de las personas morales de conformidad con lo dispuesto en el artículo 19-A de este Código, se requerirá el poder previsto en dicho artículo.
>
> La comparecencia previa a que se refiere este artículo también deberá realizarse

cuando el Servicio de Administración Tributaria proporcione a los interesados los certificados, cuando actúe como prestador de servicios de certificación."

Estos párrafos del artículo 17-D del CFF muestran el proceso de verificación de datos personales que se realiza para la emisión de certificados electrónicos y de la firma electrónica. Estos procedimientos nos muestran la disparidad de condiciones entre la recolección de datos personales para personas físicas y para personas morales, en el que las personas físicas, como ya se había mencionado, tienen que acudir de forma personalísima, mientras que para las personas morales el trámite se puede realizar por medio del representante legal y sólo se requiere de la representación legal acreditada a través de poder notarial y demostrar que cuentan con su *e.firma* lo cual es suficiente para representar grandes intereses y movimientos fiscales superiores en un buen porcentaje a los de las personas físicas, independientemente del régimen. En algunos casos dado que las personas morales pueden estar representadas por una persona, también la *e.firma* hace referencia no a una persona en lo particular.

Todos estos datos en posesión del SAT, dice el artículo 17-D que "formarán parte del sistema integrado de registro de población, de conformidad con lo previsto en la Ley General de Población y su Reglamento, *por lo tanto, dichos datos no quedarán comprendidos dentro de lo dispuesto por los artículos 69 de este Código y 18 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental"* [cursivas añadidas]. Esta disposición es una de las excepciones a la confidencialidad de la información personal en posesión del SAT.

El artículo 69 del CFF en general establece[46] las reservas a la confidencialidad de la información, mismas que se muestran en el anexo a esta investigación, pero que en general se refieren a que la información podrá ser proporcionada a "autoridades judiciales en proceso de orden penal o a los tribunales competentes que conozcan de pensiones alimenticias", así como cuando se "requiera intercambiar información con la comisión Federal para la Protección contra Riesgos Sanitarios de la Secretaría de Salud". Tampoco aplica la reserva cuando la "Comisión Federal de Competencia Económica o el Instituto Federal de Telecomunicaciones" requieran información para "calcular el monto de las sanciones relativas a ingresos acumulables en términos del Impuesto Sobre la Renta (ISR)".

Asimismo, "por acuerdo expreso del secretario de hacienda y crédito público se podrán publicar los siguientes datos por grupos de contribuyentes: nombre, domicilio, actividad, ingreso

[46] Si se desea profundizar en el Artículo 69 del CFF o en el 18 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, ver el anexo 1.

total, utilidad fiscal o valor de sus actos o actividades y contribuciones acreditables o pagadas" (artículo 69, CFF) y, entre otras disposiciones más. También se podrá proporcionar la información de los contribuyentes al Instituto Nacional de Estadística y Geografía. Este artículo también menciona el procedimiento general para que en caso de que se hayan publicado sus datos en medios electrónicos, se pueda interponer una inconformidad para la eliminación de la información publicada.

Por otra parte, el artículo 18 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG) señala lo siguiente: "como información confidencial se considerará: I. La entregada con tal carácter por los particulares a los sujetos obligados, de conformidad con lo establecido en el Artículo 19, y II. Los datos personales que requieran el consentimiento de los individuos para su difusión, distribución o comercialización en los términos de esta Ley. No se considerará confidencial la información que se halle en los registros públicos o en fuentes de acceso público". Esta disposición estaba vigente hasta la reforma de 2016, donde se aprueba la Ley General de Transparencia y por lo tanto cambia la disposición normativa.

Para finalizar es necesario subrayar que en el artículo 32 del Reglamento Interior del Servicio de Administración Tributaria, se establece que:

> "compete a la Administración General de Servicios al Contribuyente: IV. Llevar el registro de contribuyentes que obtengan el certificado digital que confirme el vínculo entre el firmante y los datos de creación de la firma electrónica avanzada, así como realizar cualquier otro acto relacionado con los mismos, incluyendo las autorizaciones relacionadas con la expedición de documentos digitales."

Como se puede observar, existe un mecanismo de procedimiento complejo en la recolección, uso, tratamiento y trasferencia de datos en el sector público, principalmente el ámbito que nos compete en este análisis, el padrón de contribuyentes, específicamente para la *e.firma* por parte del SAT. La complejidad de este caso nos obliga a consultar un amparo promovido en 2007 en materia Constitucional y Administrativa, en el que se resolvió que el "hecho de que el Código Fiscal de la Federación no establezca su definición no viola la garantía de legalidad".[47]

La tesis declara lo siguiente:

El artículo 17-D del Código Fiscal de la Federación establece que cuando las

[47] Época: Novena Época. Registro: 171757. Instancia: Segunda Sala. Tipo de Tesis: Aislada. Fuente: Semanario Judicial de la Federación y su Gaceta. Tomo XXVI, agosto de 2007. Materia(s): Constitucional, Administrativa. Tesis: 2a. XCVII/2007. Página 638.

> disposiciones fiscales obliguen a presentar documentos, éstos deberán ser digitales y contener una firma electrónica avanzada del autor, salvo los casos previstos en el propio precepto, y que para esos efectos deberá contar con un certificado que confirme el vínculo entre un firmante y los datos de creación de una "firma electrónica avanzada", expedido por el Servicio de Administración Tributaria cuando se trate de personas morales y por un prestador de servicios de certificación autorizado por el Banco de México cuando se trate de personas físicas, mediante el cumplimiento de ciertos requisitos, entre ellos, el de la comparecencia del interesado o de su apoderado o representante legal en caso de personas morales, con la finalidad de acreditar su identidad. De lo anterior se concluye que no se viola la garantía de legalidad contenida en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, por el hecho de que el Código Fiscal de la Federación ***no establezca una definición particular de lo que debe entenderse por "firma electrónica avanzada***", pues del indicado numeral 17-D se advierte el propósito perseguido con ésta, el cual, además de identificar al emisor de un mensaje como su autor legítimo, como si se tratara de una firma autógrafa, garantiza la integridad del documento produciendo los mismos efectos que las leyes otorgan a los documentos con firma autógrafa, teniendo el mismo valor probatorio; lo anterior, en razón de que la firma electrónica avanzada está vinculada a un certificado expedido por una autoridad, en este caso, por el Servicio de Administración Tributaria, en el que constan los datos del registro respectivo.
>
> Amparo en revisión 262/2007. Radio XEAGS, S.A. de C.V. 13 de junio de 2007. Cinco votos. Ponente: Sergio Salvador Aguirre Anguiano. Secretario: Óscar Zamudio Pérez.

A partir de este análisis no se encontraron las bases conceptuales y normativas suficientes que sustenten el principio de legalidad de este uso de datos en la *e.firma* del SAT. Por ejemplo, se dice que la ley de la firma no aplica en materia fiscal, pero sin embargo es utilizada en la materia fiscal para las personas físicas y morales. Existe desproporción en la recolección de la información personal por parte del SAT, pues las personas físicas son las afectadas porque a ellas son a las que se les pide su información biométrica personal: iris ocular, imagen facial y huellas dactilares. Este hecho resulta inequitativo en el trato y desproporcional en términos de la información que se solicita para quienes emiten certificados electrónicos, en términos de si es persona moral o física. La recolección de datos por parte del SAT para los certificados digitales (no específicamente para la *e.firma*), según la entrevista realizada a Fernando Martínez y según el CFF dicen que su fundamento es la Ley General de Población y dice que formará (formará es un término ambiguo

porque puede implicar que en algún momento –futuro– estará contenida en las bases de datos o que en lo inmediato pasa a ser parte de la base de datos de identidad de la Secretaría de Gobernación).

En relación con los datos de identidad es la SG la facultada, según la LGP, quien aplica las normas de la ley; sin embargo, no es la SG quien de manera directa y específica realiza esta recolección de datos biométricos para los certificados electrónicos, sino el SAT. Aquí es importante recordar que en las evaluaciones de impacto a la privacidad realizadas por la consultoría internacional dirigida por el Dr. José Luis Piñar originaron que la cédula de identidad para la población mexicana se detuviera, toda vez que no lograron acreditar la seguridad de los datos personales (José Luis Piñar, entrevista personal, 2 de octubre de 2014). En este sentido, la recolección de datos está limitada para la SG en términos de los datos de identidad para la cédula de identidad.

Los argumentos dados permiten concluir que la recolección y el tratamiento de datos personales por la *e.firma* carecen del principio de legalidad. El SAT no está facultado para ello y el uso de datos no tiene fundamento y motivo legal, lo cual es violatorio de la garantía de legitimidad de la autoridad (competencia) contemplada en el art. 16 constitucional, lo cual es objeto de amparo. No tiene fundamento legal dicha recolección ya que la ley exceptúa para efectos fiscales la aplicación de esta y, como consecuencia, la recolección de los datos biométricos que señala la Ley General de Población tampoco es competencia del SAT. Como consecuencia, los datos personales que incluyen dicha recolección no están exceptuados como datos personales de acuerdo a la LFTAIPG.

La recolección de datos personales por parte de la autoridad administrativa (SAT), como cualquier otro acto administrativo, debe ser realizado por autoridad competente y fundado en un ordenamiento legal vigente, (artículo 4 de la Ley Federal de Procedimiento Administrativo).

En el siguiente análisis se profundiza el caso con base en los principios de protección de datos personales, contenidos en los tratados internacionales suscritos por México.

4.7 Análisis a partir de los principios generales de protección

Los principios para el manejo y tratamiento de los Datos Personales son obtenidos de diversas disposiciones jurídicas nacionales e internacionales, dentro de los cuales encontramos al Convenio 108 de APEC, Directiva 95, Resolución de Madrid y Marco de Privacidad de APEC. Algunos de estos principios son: la licitud, el consentimiento, la información, la calidad, la finalidad, la

lealtad, la proporcionalidad, la respetabilidad, la seguridad y la confidencialidad.

Lina Ornelas y José Luis Piñar (2013: 39) establecen que "los principios son uno de los vértices sobre los que gira un sistema de protección de datos personales, mismos que se convierten en obligaciones para el responsable que trata los datos personales, obligado a velar y garantizar que el tratamiento sea licito y legítimo". Recordando que todo tratamiento tiene excepciones. Para el caso de México están comprendidas en la CPEUM en su artículo 16, de la siguiente manera:

> "toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de estos, 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*".

De acuerdo con el capítulo 2 se realiza este análisis, en el cual se dijo que los principios tanto para el sector público como para el privado varían y sistematizándolos podrías decir que son los siguientes.

Cuadro 12. Principios aplicables

SECTOR PRIVADO	SECTOR PÚBLICO
- Licitud - Consentimiento - Información - Calidad - Lealtad - Proporcionalidad - Respetabilidad - Seguridad - Confidencialidad	- Licitud - Calidad de datos - Acceso y corrección - De información - Custodia y cuidado de la información - Consentimiento para la transmisión

Fuente: elaboración propia, con datos hasta diciembre de 2015.

En este sentido, resulta importante diferenciar los principios en dos esferas: pública y privada, y encontrar las unidades analíticas para conocer a profundidad y de la manera más objetiva el caso.

Lo primero que surge al ver la lista diferenciada entre los principios de privacidad entre una esfera es la disparidad en principios que rigen el uso y tratamiento de datos en un sector y en otro. De inicio, contar con unos principios para un espacio y para otro, implica una diferenciación de significado y sentido de la protección en un ámbito y en otro. Esto origina por lo tanto una incongruencia en las leyes en la materia. El mensaje manifiesto en la norma, a partir de esta diferenciación de principios permite observar que en el sector privado existe una regulación más

amplia y que para el sector público esta protección es menor o deficiente. Esto va en contra de los principios que rigen el Estado liberal que tienen como premisas la libertad, la seguridad de la vida y de las posesiones. Así como en contra de las garantías y derechos humanos de las personas al dejar de lado la universalidad de la protección.

Es decir, el hecho de que sea legal, y que vaya acorde con las normas establecidas, no implica que esa norma establecida tenga una base fundada y motivada en los principios jurídicos y éticos universalizables, dice Peter Singer (1995).

Como se puede observar, en el manejo privado de los datos personales se incorporan más principios en comparación con el manejo de la información personal en el sector público. Los principios reconocidos por la LFPDPPP son nueve: licitud, consentimiento, información, calidad, lealtad, proporcionalidad, responsabilidad, seguridad y confidencialidad. Y para el sector público se reconocen: la licitud, la calidad de datos, el acceso, la corrección, la información, la custodia, el cuidado de la información y el consentimiento para la transmisión. En lo consecuente se analizará principio por principio con el fin de conocer sus implicaciones, mismas que permitirán realizar un análisis superior en el siguiente capítulo.

Licitud

El principio de **licitud** implica que el tratamiento de los datos debe llevarse a cabo de forma leal y lícita; es decir, con pleno cumplimiento de la legalidad y el respeto de la buena fe y los derechos del individuo, cuya información es sometida a tratamiento. En "todo tratamiento de datos personales debe efectuarse de forma lícita y leal con respecto al interesado; que debe referirse, en particular a datos adecuados, pertinentes y no excesivos en relación con los objetivos perseguidos, explícitos y legítimos" (Piñar y Ornelas, 2013: 44). Según estas definiciones la licitud está relacionada con la "legalidad" (cumplimiento de la ley) y con el respeto de la buena fe.

Como se puede observar en el caso de la información obtenida por el SAT para la *e.firma* de las personas físicas, el principio de licitud se atendió de manera deficiente, alejado "de los datos adecuados, pertinentes y excesivos", por tres situaciones: primero porque sólo se solicita y exige su uso a un tipo de contribuyentes, luego porque la recolección está dirigida a verificar la identidad del contribuyente (función que tiene asignada la Secretaria de Gobernación y no el SAT) y finalmente porque en ninguna otra base de datos pública se toman tantos datos como para la *e.firma* del SAT para las personas físicas, dentro de la cual se incluye información biométrica de alta sensibilidad. Aquí debemos agregar que el porcentaje de contribuciones supera por mucho a

aquellas que no son obligadas a utilizar la *e.firma* como herramienta de verificación de identidad y transacciones electrónicas. En este sentido, el tratamiento para la *e.firma* carece de licitud

Consentimiento

Este principio es de suma importancia. En el primer y tercer capítulo de esta investigación se analizó cómo el diseño de la protección de datos personales en México estuvo orientado en gran medida por este principio. Es decir, una de las grandes discusiones y debates que se llevaron entre los diferentes participantes del sector privado y gubernamental fue el consentimiento. Bueno, este principio resulta fundamental para desvincularse de responsabilidades ante el uso de los datos por parte de quienes los posean.

En este sentido, dice José Luis Piñar y Lina Ornelas (2013: 45) que "como regla general, el responsable deberá contar con el consentimiento del titular para el tratamiento de sus datos personales. La solicitud del consentimiento deberá ir siempre ligada a las finalidades concretas del tratamiento. Para el caso de los privados esta finalidad debe estar definida en el aviso de privacidad". El consentimiento, agregan los autores, "deberá utilizarse para tratar los datos personales para finalidades específicas, no en lo general". Esto quiere decir que al solicitar el consentimiento para el tratamiento de datos personales el responsable deberá anunciar para qué utilizará la información de manera específica, para el caso del tratamiento en posesiones de los particulares.

Qué sucede en el caso de la información de la *e.firma* para el SAT. Dicen los lineamientos aplicados para la protección de datos personales por parte del sector público que "toda transmisión de datos personales deberá contar con el consentimiento del Titular de los datos, mismo que deberá otorgarse en forma libre, expresa e informada, salvo lo dispuesto en el lineamiento vigésimo segundo. (INAI, 2016: 58)

> Donde se dice que "las dependencias y entidades podrán transmitir datos personales sin el consentimiento del titular de los datos, en los casos previstos en el artículo 22 de la Ley. Asimismo, deberán otorgar acceso a aquellos datos que no se consideren como confidenciales por ubicarse en los supuestos establecidos en los artículos 7, 12 y 18." (INAI, 2016: 58.)

Las disposiciones de los artículos 7, 12 y 18 hacen referencia a los datos personales que se encuentren en las instituciones públicas obligadas a hacerlos públicos. Es información pública de

oficio. En el artículo 7 se enlista la información que las dependencias deben hacer pública, como por ejemplo su estructura orgánica, los servicios que ofrecen, los tipos de contrataciones que celebran, etc. El artículo 12 dice que los sujetos obligados publicarán a quien entreguen recursos públicos, y el artículo 18 hace referencia a la información que se encuentre en los registros públicos o fuentes de acceso público.

El asunto del consentimiento en términos de la *e.firma* en el SAT según la entrevista realizada a Fernando Martínez Coss (19 de agosto de 2016) dice que efectivamente el SAT solicita el consentimiento del titular de los datos al firmar la solicitud de emisión de la *e.firma*. La leyenda dice lo siguiente:

> "Que es de mi conocimiento y conformidad que con el propósito de brindar seguridad jurídica en la obtención y uso del Certificado de Firma Electrónica Avanzada, se debe garantizar la existencia del vínculo jurídico entre el Certificado de Firma Electrónica Avanzada y su titular, acreditando plenamente en el proceso de emisión del certificado la identidad de la persona física titular, o bien la identidad de las personas físicas en su carácter de representantes o apoderados en el caso de personas morales, por lo cual deberé comparecer de manera personal ante el SAT en donde se obtendrán y almacenarán mis datos de identidad consistentes en el registro electrónico de datos biométricos como son huellas digitales, fotografía, captura de la imagen de los iris y mi firma autógrafa, ***asimismo deberá realizar el registro electrónico de la documentación que acredita mi identidad***. De la misma forma me manifiesto conocedor de que los datos de identidad mencionados en este numeral formarán parte del Sistema Integrado de Registro de Población, de acuerdo con lo dispuesto por el noveno párrafo del artículo 17-D del Código Fiscal de la Federación, así como las disposiciones conducentes de la Ley General de Población y su Reglamento. (SAT, 2016)

En el párrafo anterior se logra leer que además de los datos biométricos se deberá realizar el registro electrónico de la documentación que acredita la identidad. En este sentido los datos que acreditan la identidad son diferentes a los datos biométricos y entonces la pregunta sería y para qué se recaban datos biométricos si la información de identidad no es ésta.

En este mismo artículo 17, apartado G se lee que el correo electrónico integrado al certificado de la firma electrónica avanzada será de carácter público. En este sentido, la recomendación sería crear un correo electrónico desvinculado de otros datos personales para que

la publicidad de ese dato personal no afecte la privacidad de las personas.

Como podemos observar, el consentimiento en realidad no propiamente es un "consentimiento", sino un aviso de obligatoriedad ante la necesidad de cumplir con una obligación o requisito económico y social. Es decir, si fuera consentimiento estaría salvado el derecho de autonomía, voluntad, libertad e implicaría la posibilidad de salvaguardar otros derechos (garantías) de la persona. Este "consentimiento" es en realidad un requisito de obligatoriedad para acceder a un servicio o un bien, de tal manera que si la persona no firma el servicio no le es otorgado y por tanto se presenta la indefensión o falta de atención ante una negativa del uso, manejo y protección de la información personal. Esta situación pasa tanto en el sector privado, como en el público.

Información

Este principio tiene el objetivo de incorporar el instrumento del "aviso de privacidad" como un medio para informar "de los términos a que sujeta el tratamiento de sus datos personales y, en su caso, recaba el consentimiento necesario. Por tanto, es también un deber u obligación del responsable" (Piñar y Ornelas, 2013: 45-56). Este instrumento ha sido implementado en el ámbito del sector privado, pero no para el sector público. En el ámbito del sector público existe lo que en el lineamiento decimoctavo se denomina: "formato para informar al titular".

Este principio permite a las personas conocer el tipo, modo y procedimiento para el tratamiento de sus datos personales, lo cual le permitirá ejercer los derechos y garantías para su protección. En este sentido, para la efectividad de este principio se requiere que exista especificidad en los procedimientos de recolección y tratamiento. El modelo de formato para informar a los titulares de datos personales en posesión del sector público debe incorporar la siguiente información: tipos de datos recabados, sistema donde se tratarán, fundamento, finalidad, lugar de registro de la base de datos, casos donde se transferirán datos, la unidad responsable del sistema, dirección para ejercer derechos que correspondan (INAI, 2005: 59).

En relación con la información de la *e.firma*, sin duda algunos aspectos son contenidos en su generalidad en el apartado dos de la solicitud. Sin embargo hace falta informar de manera clara sobre cuál es su tratamiento, así como el responsable de la protección de los datos recolectados y mencionar que al recolectar datos sensibles se deberán tomar otros mecanismos de protección administrativos, legales, técnicos y tecnológicos de calidad superior, si fuera necesario, a los dictados por la norma, porque dice que serán protegidos con las normas de seguridad del Banco de México, pero en la misma solicitud se deslinda de responsabilidad al Banco de México sobre

este procedimiento de protección.

Calidad

Para considerar calidad en los datos, se deben especificar datos verídicos y exactos, para que se "refleje realmente de forma fiel la realidad de la información tratada" (Piñar y Ornelas. 2013: 46). En este principio cabe agregar, por ejemplo, un aspecto que Fernando Martínez Coss (entrevista realizada el 19 de octubre de 2016) comentaba sobre la calidad de la información, como parte del argumento de la necesidad de recolectar información biométrica para la *e.firma*. Él hizo énfasis en la necesidad de "acreditar la identidad", ya que en 1996 por acuerdo presidencial se publicó en el Diario Oficial la disposición de que la CURP debería ser usada y adoptada por toda la Administración Pública Federal, sin embargo, afirmó que cuando necesitaron confrontar el RFC del SAT con la CURP, ya que tiene que existir coincidencia entre "el Registro Nacional de Población, la CURP y con el Registro Federal de Contribuyentes", se percataron que "la información no era de buena calidad y había diferencias. Esas diferencias en una situación de servicios o dotación de servicio digital, enfrentaría el repudio, porque al haber diferencias de personalidades, legalmente se puede repudiar el acto, entonces, ahí fue donde se tomó la decisión: necesitamos rehacer el Registro Federal de Contribuyentes".

Es importante aclarar que, si bien la información no tenía calidad y era necesario "rehacer el RFC", esto no implicaba que deberían solicitar información biométrica, sobre todo porque para la emisión del RFC no son necesarios estos datos de máxima protección y sensibilidad.

Finalidad

El principio de finalidad atiende la necesidad del fin u objetivo del tratamiento. Es decir, los datos deben ser recolectados y tratados para una finalidad específica y no para múltiples finalidades, las cuales deben ser explícitas, legítimas y relacionadas con la actividad del responsable. Sin embargo, dice la norma que sí, para el caso de los datos en posesión de los particulares, se trata la información según el aviso de privacidad, entonces es legal y acorde con la norma. Sin embargo, la pregunta que surge aquí es: si el aviso de privacidad habla de tratar la información de manera diferenciada a las normas constitucionales, lineamientos u otras normas, o si incluso su tratamiento va en contra no necesariamente de las normas constitucionales o nacionales, pero sí en contra del sentido original de la protección, la libertad, la autonomía, por qué sólo va dirigida a la

obligatoriedad de aceptar el uso y tratamiento.

Otra de las premisas en este principio es: una vez que haya caducado el fin previsto en el informe o aviso de privacidad la información debe cancelarse, borrarse y eliminar el registro. Este hecho también debería manifestarse al titular de los datos.

Sobre la información de los datos para el uso de la *e.firma* se tiene, tal como se analizó en el principio anterior, que en la solicitud para la *e.firma* en el apartado de términos y condiciones se informa sobre el uso y tratamiento de los datos personales. Sin embargo, esta información carece de claridad y no va más allá de ser un proceso "informativo", ya que dicho proceso de información está relacionado con la transparencia, es decir, con hacer del conocimiento del titular de los datos los modos, maneras, tipos y en general especificidades sobre el uso de la información. Se trata de que el titular tenga claridad sobre dónde se guardan los datos, quién los tiene, cuál es el fundamento legal, la necesidad de dar los datos biométricos y si tanto el SAT como la SG tienen facultades legales y legítimas para realizar esta recolección de datos, si es o no excesiva esta recolección y porque sólo a ciertas personas con el régimen de personas físicas se les exige este requerimiento. Como se puede ver este principio es cumplido de manera deficiente.

Lealtad y expectativa razonable de privacidad

Piñar y Ornelas (2013:51) al tratar estos principios (para el caso de la protección de datos en posesión del sector público) señalan que el tratamiento debe ser "lícito y leal", y la primera pregunta que surge es: ¿y qué tiene que ver el principio de licitud, con la lealtad y la expectativa razonable de la privacidad?, pues a simple vista cada concepto (principio) atiende aspectos diferenciados, aunque tanto Piñar como Ornelas se introducen a la "licitud", es importante más bien dirigir la discusión propiamente a la "lealtad" y luego a la "expectativa razonable" para entender el origen de lo que esto implica y cómo se ha aplicado a los datos personales.

La lealtad, dice la Real Academia de la Lengua Española (2016) proviene de leal y ésta a su vez del latín "legālis" que significa "que guarda a alguien o algo la debida fidelidad", o que algo es "fidedigno, verídico, fiel, en el trato o en el desempeño de un oficio o cargo", así como también se dice leal como acción cuando es "propio de una persona fiel". En este sentido, lealtad (que alude a leal) es el "cumplimiento de lo que exigen las leyes de la fidelidad y las del honor y hombría de bien" o también definida como "legalidad, verdad y realidad". Atendiendo a estas consideraciones, entonces el principio de lealtad es un principio que implica "fidelidad", "veracidad", "realidad", "honor" y "bien" en el tratamiento de los datos personales por parte de terceros, y si estos

principios derivados de la lealtad que se manifiesta no por el titular de los datos, sino por quien trata datos personales no se presentan en el "ejercicio de su desempeño, oficio o cargo al tratar esos datos", entonces se estaría incumpliendo este principio.

Ornelas y Piñar (2013: 51) al continuar revisando este principio dicen que "la obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos". Se dice que existe actuación fraudulenta o engañosa cuando "exista dolo, mala fe o negligencia en la información proporcionada al titular sobre el tratamiento; se vulnere la expectativa razonable de privacidad de titular a la que refiere el artículo 7 de la LFTAIPG o que las finalidades no son las informadas en el aviso de privacidad" (Piñar y Ornelas, 2013: 51).

En este sentido se hace también referencia "a la confianza", tal como ya lo hemos mencionado. Sin embargo, ellos agregan: "el mutuo acuerdo establecido en el contrato" (ya que aluden a los datos en posesión de los particulares" y aquí vuelve a entrar un tema de importancia para los datos personales: el consentimiento, del cual ya hemos hablado y abundaremos un poco más en las Conclusiones. Sobre este punto es necesario aclarar que, si la información del acuerdo o contrato que se firma es confusa o poco clara, así como el uso de esta información, la transferencia y hasta la licitud de este tratamiento, entonces nos encontramos con un conjunto de principios débilmente aplicados en materia de datos personales y más aún en el ámbito público. También aparece lo que se conoce como "error en el consentimiento", que justo identifica que puede existir "una falsa apreciación de la realidad por una de las partes y que provoca que el consentimiento no se otorgue de manera libre, ya que se desconocen todas las situaciones del caso" (Olea, 2007:94); por ejemplo, en relación con la información biométrica que recolecta el SAT en principio la mayoría de las personas parte de que es "leal", "lícito", "legal" y que se cumple con los principios de "licitud", "consentimiento", "de información", pero la realidad es que éstos son procedimientos complejos en sus explicaciones y que un ciudadano común desconoce por ser un conocimiento especializado, lo cual no significa que por dejar los datos personales esta dependencia cumpla con estos principios porque en realidad no está obligada a éstos, ya que son principios que en México sólo aplican al caso de la posesión de datos por parte de los particulares.

En tal sentido, este principio, al igual que los anteriores, son indispensables en el tratamiento de datos personales. El asunto aquí es que se está partiendo de que el uso de estos datos es una necesidad tanto para el sector privado como para el sector público. La legislación para el sector privado fue creada con mayor detalle y urgencia, derivado de la necesidad económica y de innovación y la relación transfronteriza de los datos personales, así, como con el reconocimiento de

las afectaciones a la economía en caso de no proteger los datos personales, y a la vez de incentivar el uso lícito de éstos.

Sin embargo, tanto para el tratamiento de datos personales para el sector público como para el privado es necesario hacer congruentes los criterios. Se protege a un mismo sujeto de derecho en dos diferentes ámbitos y esta protección es diferenciada, motivo por el cual se parte de una falta de congruencia en los principios aplicados tanto en el discurso como en la realidad.

Dicen Piñar y Ornelas (2013: 51), sobre la "expectativa razonable" que "se trata de una presunción que debe ser valorada utilizando un estándar objetivo, es decir, considerando la expectativa de privacidad que tendría una persona media. Por lo tanto, no es la expectativa de privacidad que pueda tener cada persona, ya que se trataría de un estándar subjetivo que varía en función de cada titular de los datos, sino de la expectativa de privacidad que puedan tener objetivamente los titulares de los datos en atención a diversos factores, tales como la normatividad aplicable, la evolución tecnológica y social, así como el grado de cultura en la protección de datos personales que haya en el país.

Aquí los autores aluden a que se trataría de encontrar un estándar medio que permitiera la protección de diferentes racionalidades. El asunto aquí es cómo todo en la realidad social se argumenta, construye y legitima (Berger y Luckmann, 1996), estas creaciones con regularidad están vinculadas a ciertos intereses, que para el caso de México fueron los intereses de quienes lograron posicionar su voz en el Congreso de la Unión y velar por las menores afectaciones posibles a sus intereses, o lograr acuerdos derivados de amplias negociaciones entre básicamente algunos grupos de empresarios, el gobierno y el IFAI, donde la ciudadanía tuvo muy poca participación. Por lo tanto, hicieron uso de esta "expectativa razonable" para dejar "la libre regulación del sector privado" en materia de datos personales, y además para el sector público se dejó con una mínima regulación, ya que "por disposiciones públicas" este tratamiento puede quedar alejado de los principios que la misma Constitución reconoce.

Otro aspecto relacionado con la "expectativa razonable" es cuando se dice que el tratamiento de datos obtenidos a través de fuentes de acceso público respetará la "expectativa razonable de privacidad", a que se refiere el tercer párrafo del artículo 7 de la Ley" (Piñar y Ornelas, 2013: 51). Aquí de la misma manera se deja a los libres principios de aquellos que toman los datos personales sólo por considerar "de acceso público" y aquí las preguntas son: ¿y quién define lo que es público y lo que es privado? Hannah Arendt (2007) dice que, en las sociedades modernas, el mercado, la fuerza y la violencia del Estado son quienes definen la separación entre

lo público y lo privado, donde más bien se ha originado una confusión entre ambos espacios.

Proporcionalidad

Los datos deben ser necesarios, adecuados y relevantes para los fines que en origen tiene la necesidad del tratamiento. En concreto, el Artículo 45 indica lo siguiente: "Sólo podrán ser objeto de tratamiento los datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las que se hayan obtenido" (INAI, RPD). Por lo tanto, "tratar datos personales que no son necesarios, adecuados o relevantes en atención a la finalidad de dicho tratamiento, supondría incumplir con este principio" (Piñar y Ornelas, 2013: 53).

Al respecto, para cada recolección son los datos mínimos los que deben preponderar y para el caso de los datos biométricos en el SAT deberíamos preguntarnos si se está atendiendo esta consideración de "los datos mínimos", donde "la minimización adquiere especial relevancia en el caso de los datos personales sensibles… en atención a su naturaleza y la necesidad de una mayor protección" (Piñar y Ornelas, 2013: 53).

El argumento del SAT para el uso de los datos biométricos atiende a la necesidad de "identidad"; sin embargo, el SAT no tiene la facultad para acreditar la identidad. Quien en origen debería tener esta facultad es la Secretaría de Gobernación, sin embargo cuando se pretendió realizar el principal instrumento de identidad (la cédula de identidad), se realizaron estudios sobre privacidad y se concluyó que no se contaban con las medidas para continuar con este procedimiento de identidad, sin embargo el SAT sí está cumpliendo para algunas personas, las que menos impuestos pagan, con asegurar la identidad por medio de las huellas digitales, el iris ocular y la imagen facial. La normativa sobre protección de datos en posesión de los particulares también admite que sí existe disociación o anonimización de los datos, de tal manera que no se pueda identificar a los titulares de los datos, entonces la ley no aplica, ya que no se estaría en la posibilidad de identificar a los titulares de esos datos. Situación que también debería aplicar para el caso de los datos en posesión de los particulares.

Ante esto último existe una propuesta que deriva justo de la disociación de datos y anonimización de los mismos, a partir de cada una de las facultades de las dependencias de gobierno y que se explicará al finalizar este capítulo.

La responsabilidad

Este principio proviene del principio de *"accountability"* que en México se ha traducido como "rendición de cuentas" y que para el caso de la protección de datos personales se considera como "responsabilidad". Este principio está reconocido por la normatividad internacional, pero también por la ley de datos personales en posesión de los particulares en México (LFPDPPP). Dicen Piñar y Ornelas (2013: 55):

> "este principio es la verdadera garantía para el titular de los datos quien deposita su confianza en el responsable, mismo que deberá tomar todas las previsiones para que los datos sean tratados de acuerdo con la voluntad del dueño de la información y bajo las medidas de seguridad que se prevean para la vía contractual. Así, dado que existe un tráfico de datos intenso y en muchas ocasiones este se da fuera de las fronteras de nuestro país, el ciudadano tendrá la tranquilidad de que, si su información ha trascendido a manos de terceros en otras latitudes, éste estará enterado de las cautelas con que debe tratar su información".

Con este principio se vuelve a verificar la tendencia a la "autorregulación" de los datos personales en posesión de los particulares, considerando que se debe contar con las medidas necesarias: técnicas, administrativas, tecnológicas, éticas y legales para cumplir con este principio, el cual también contempla sanciones económicas y penales. Además de esto, lo interesante también radica en que la Organización de las Naciones Unidas se ha pronunciado al respecto señalando que "en caso de violación de las disposiciones de la ley nacional, así como de los principios mencionados, deberán preverse sanciones penales u otros recursos apropiados" (Piñar y Ornelas, 2013: 55). Estas sanciones, que van más allá de una amonestación económica, responsabilizan incluso penalmente a quienes hayan tratado datos personales sin respetar lo que marca la ley y con base en los principios aquí señalados se puede hacer acreedor a sanciones del tipo penal. Lo cual resulta sin duda un elemento importante de considerar, pero también para el caso del manejo de datos en posesión del sector público.

Estos son los principios que se contemplan para la protección de datos personales en la normativa internacional, en la de protección de datos personales en posesión de los particulares en México, pero no para la protección de los datos personales por parte del sector público en México, primero porque la regulación para el sector público es mucho menor, sólo contempla lo descrito en la Constitución con la condición de que no se aplicará tal artículo cuando sea por disposición pública, y este texto va en contra de todos los principios de protección de datos personales que

tanto la regulación internacional como la de otros ámbitos promueven. Con esto se está dejando desprotegida a la persona bajo los designios de las disposiciones públicas de los Estados y los gobiernos en turno. De allí la necesidad de profundizar en este tema de la protección de datos con otros principios que nos den elementos, herramientas y mecanismos para incorporar una normativa, ciertos límites que permitan la protección de la persona y el ciudadano, contemplando las necesidades del mercado y del gobierno sobre los datos personales.

Principios del reglamento europeo de protección de datos

La regulación en materia de datos personales en el sector público y privado se ha dejado de lado, especialmente en el sector público. A la fecha está detenida la propuesta de "Ley General de Protección de Datos Personales" en el Senado de la República. Esta podría ser una excelente oportunidad para incorporar elementos en los ámbitos privado y público, donde se logren aciertos que, si bien permitan la innovación, la competitividad y el crecimiento del mercado, lo hagan con una base solidad de principios, derechos y normas que protejan con amplio sentido de ética y responsabilidad a las personas en México.

Esta no es una simple situación que requiera la participación de diputados, senadores, algunos funcionarios del INAI y ciertos sectores empresariales implicados. Se requiere debatir un problema público de alto impacto que tiene y tendrá implicaciones en muchos sectores económicos, sociales y políticos. Es necesario, por lo tanto, llamar a la sociedad a la discusión pública a debatir un asunto de importancia nacional, pues a partir de su definición serán las soluciones definidas y consideradas.

El Reglamento europeo de protección de datos personales viene a sustituir a la Directiva 95/46/ CE. Este Reglamento tuvo una amplia discusión en el Parlamento Europeo y fue aprobado el 14 de abril de 2016 y publicado el 04 de mayo del mismo año. El Reglamento aumenta los controles en el uso de los datos para fines judiciales y policiales, incorpora innovaciones como la figura del delegado de protección de datos personales. El Reglamento entró en vigor el 25 de mayo del 2018. Todos los países disponen de dos años para trasladar los cambios de la directiva a la legislación nacional, asimismo este Reglamento se dice de alcance general, obligatorio para todos los Estados miembros y ninguno podrá adoptar medidas contrarias a la efectividad del mismo. Entre las disposiciones con mayor relevancia que podrían incorporarse a la legislación mexicana están las siguientes:

- El derecho a la rectificación o supresión de los datos personales: derecho al olvido.

- Necesidad de consentimiento claro y afirmativo.
- La portabilidad: derecho a trasladar los datos a otro proveedor de servicios. Por ejemplo, si tus datos los tiene *Google* y ahora quieres pasarte a *Yahoo!*, el primero deberá trasladarlos a este último, con una solicitud de por medio.
- Derecho a ser informado si los datos personales han sido vulnerados, copiados o robados.
- Notificación de violaciones de seguridad a la autoridad de control.
- Cuando sea de alto riesgo: notificar la violación de seguridad al interesado.
- Lenguaje claro y comprensible sobre las cláusulas de la privacidad.
- Multas de hasta el 4% de la facturación global de la empresa en caso de infracción.
- Existencia del delegado de la protección de datos personales.
- Responsabilidad.
- Privacidad desde el diseño.
- Privacidad por defecto.

Así como la ampliación de los principios de seguridad y tutela de este derecho humano. Según el siguiente cuadro:

Cuadro 13. Principios de seguridad y tutela

SECTOR PRIVADO	SECTOR PÚBLICO	PRINCIPIOS REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS PERSONALES
- Licitud - Consentimiento - Información - Calidad - Lealtad - Proporcionalidad - Respetabilidad - Seguridad - Confidencialidad	- Licitud - Calidad de datos - Acceso y corrección - De información - Custodia y cuidado de la información - Consentimiento para la transmisión	Artículo 5 - Licitud - Lealtad - Transparencia - Limitación de finalidad - Minimización de datos, - Exactitud, - Limitación del plazo de conservación, - Integridad y confidencialidad, - Responsabilidad proactiva, Artículo 6 - Licitud del tratamiento

Fuente: elaboración propia.

Ya no sólo se contemplan los derechos ARCO, sino los derechos ARSLPO: Acceso, Rectificación, Supresión, Limitación del tratamiento, Obligación de notificación, Derecho a la portabilidad,

Derecho a la oposición y Decisiones individualizadas. Otro de los mecanismos que son innovadores y que cambiarán el diseño organizacional de la protección de datos en la Unión Europea, pero que además se ve como una herramienta factible de implementar en México, es el Delegado de protección de datos personales.

Este delegado es designado, según lo establecen los artículos 37 al 39, por el "responsable y el encargado del tratamiento de protección de datos siempre que el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en el ejercicio de sus funciones". El delegado de datos podrá ser exigible a grupos empresariales, autoridades u organismos públicos. Los supuestos en los que es posible (u obligatorio) su nombramiento, están estipulados también en los artículos mencionados, así como su régimen, posición y funciones.

Como podemos observar, los principios en el manejo de datos personales se incrementan con este nuevo reglamento que se tardó siete años en ser aprobado. Sin duda es un gran avance. Sin embargo, este Reglamento también se queda corto cuando hablamos de la legislación en el sector público. Por lo tanto, una necesidad urgente es sincronizar principios para la protección de datos personales, tanto en el sector público como en el privado, porque no se están regulando dos aspectos de sujetos diferenciados, sino al mismo sujeto y con los mismos derechos tanto en un sector como en otro.

Es decir, se reconoce la necesidad en el uso de datos para la economía y para la provisión de servicios y el control de la nación en términos de seguridad. Entonces no es que se tenga aversión a una base de datos nacionales. Con este reglamento en el Parlamento Europeo se decidió crear un registro europeo de los pasajeros de transporte aéreo, como medida contra el terrorismo. En este mismo sentido iría la necesidad de crear una base de identidad nacional, pero que cuente primero con una definición clara de lo que se quiere atacar y resolver con esto, luego sobre las facultades de cada entidad de gobierno y del Estado. Por supuesto que se definan claramente los derechos de las personas, de las cuales no sólo están incluidos los ciudadanos, sino también toda a aquella persona de la cual se posean datos personales. Es necesario que México reconozca esta necesidad; que el Estado y el gobierno actúen en consecuencia y que la ciudadanía discuta la necesidad de definir este problema público para dar la solución más adecuada, pero siempre con derechos claros para que las personas que en última instancia resulten las más afectadas tengan las herramientas y los mecanismos necesarios para protegerse del Estado y de las grandes corporaciones económicas internacionales.

Para finalizar, en el siguiente apartado se analizan las consecuencias para el gobierno,

las empresas privadas internacionales y nacionales, contemplando su tamaño, y las consecuencias para la persona en lo particular. El análisis se realiza a partir de las categorías estudiadas. Es un capítulo que contiene reflexiones finales y que identifica aspectos importantes de considerar en sus diferentes niveles.

CAPÍTULO 5. CONSECUENCIAS PARA LOS SECTORES EN LA GESTIÓN Y PROTECCIÓN DE LOS DATOS

Toda acción gubernamental que vaya o no acompañada de la participación de otros actores tiene consecuencias importantes. Dichas consecuencias y/o implicaciones reconocen una relación de causa-efecto, que manifiesta los vínculos políticos, económicos y sociales presentes en los actos de gobierno. Estos actos suelen presentarse sin una conciencia clara de los efectos de una decisión, haya sido consensuada o no. En este último capítulo se analizan las consecuencias, es decir las causas y el efecto de algunas unidades analíticas de la protección de datos personales en México. Las unidades analíticas, las causas, se obtienen de la evidencia empírica en el diseño institucional y organizacional, y sus efectos se explican con la teoría y las evidencias empíricas a partir de las entrevistas y de algunos datos estadísticos e informes oficiales. La causa son las unidades analíticas y los efectos de las consecuencias.

Tanto causas como efectos se analizan para tres actores implicados en el diseño institucional y organizacional de la protección de datos personales: el gobierno, las empresas y las personas. Aunque estas últimas no hayan participado directamente en el diseño. Entonces, en el caso del gobierno se analizan las consecuencias de los discursos, de las herramientas y los medios para la protección de datos personales. Lo mismo en el caso de las empresas y las personas.

5.1 Derechos y garantías entre procesos burocráticos

El diseño institucional dio lugar a que en México la protección de datos personales sea un derecho humano fundamental reconocido por el Artículo 16 de la Constitución, y no sólo protegido por ésta, sino por todos los tratados internacionales reconocidos por el Estado mexicano. El que haya sido reconocido como derecho humano fundamental y se le provean de garantías es un gran logro del diseño de protección de datos personales, influenciado y promovido por organismos internacionales con una acertada recepción en México. Los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) y los principios en el tratamiento de los datos provén a la persona de herramientas administrativas y jurídicas modernas, pero insertas en un contexto con muchas complicaciones prácticas y de acción directa para las personas.

El modelo de Estados Unidos sobre la privacidad la consideran ligada a tres derechos mayores: la vida, la libertad y la propiedad, y justo la regulación en materia de datos personales en México dotó de propiedad y tutela a la persona con respecto a sus datos personales. En ese sentido

se le atribuye el derecho de propiedad de sus datos, así como el manejo de comunicarlos o no —la autodeterminación—. Esta asignación formal, constitucional de la propiedad de los datos está relacionada con el derecho subjetivo, el cual implica la actuación de la persona para poder ejercerlo y hacerlo valer ante las autoridades competentes públicas o privadas. Por ejemplo, vía una queja administrativa o un juicio en la materia competente: penal, civil, mercantil o constitucional (Juicio de Amparo).

Como derecho humano puede hacerse valer y defenderse por la vía del amparo, principalmente cuando es una autoridad quien afecta estos derechos. Aunque cuando es un particular también se incluyen otros medios de defensa. Justo aquí se complica la protección para la persona porque la protección está sectorizada, dispersa y fragmentada. Es una protección que existe, pero que es complicada. Por ejemplo, como medio de protección, el Juicio de Amparo por sí mismo es positivo, pero considerando las características del sistema jurídico mexicano donde la corrupción, la impunidad (Aguilar, 2013), y la falta de credibilidad en las instituciones judiciales (Magaloni, 2007) son inherentes al funcionamiento del sistema, la acción y defensa de la persona frente a los poderes del Estado o de los particulares se debilita.

Jorge Carpizo (2009: 86) dijo que "de nada o poco sirven las declaraciones si no existen simultáneamente los procesos y procedimientos, las garantías procesales constitucionales para resarcirlos si éstos son violados", y esto es cierto, pero no es suficiente, se requiere un sistema de administración congruente, sistematizado, transversal y éticamente aplicable según el discurso que se promulga. Para el discurso de los derechos humanos se requiere un Estado que apoye en su protección, no sólo con el reconocimiento de éste, sino con las herramientas administrativas y jurídicas capaces de ser utilizadas fácilmente por las personas.

Una de las características de los derechos humanos es que debe ser universal, y como universal es el derecho, universal debe ser su protección. Sin embargo, vemos que en el caso de la protección de datos personales y de todo derecho humano todavía por la vía del amparo no se pueden proteger los derechos humanos cuando los particulares violen estos derechos, en todo caso procedería por ser un asunto entre particulares un juicio civil, penal, mercantil, administrativo u otro, dependiendo del caso a tratar. Esta situación es una de las causas que podrían denominarse negativas para las personas porque es muy claro ver, entender y comprender que la persona *por sí misma* no tiene las mismas herramientas y los mismos recursos que una corporación empresarial o que el propio Estado, en ese sentido surgen algunos problemas muy interesantes sobre la relación entre datos personales, Estado, Empresas y Personas.

El supuesto en el diseño institucional es que el Estado crea todo un conjunto de controles por medio de normas, valores, principios, procesos, autoridades de control, multas y sanciones. Herramientas que enriquecen con las medidas de autorregulación y buenas prácticas por parte de particulares, como certificaciones y diversas herramientas de seguridad informática para dar certidumbre al manejo de datos y garantizar que el tratamiento de datos está siendo tratado de manera lícita y con base en los principios estipulados en las normas establecidas, sin embargo todos estos nuevos procesos y herramientas tanto en el sector privado como en el público, primero generan para el individuo una dispersión en el manejo de sus datos y dificultad para protegerlos, pero al mismo tiempo que lo proveen de herramientas en el sector público, también para el sector público se prevén garantías y mecanismos de defensa como el Amparo. Pero para el caso de los particulares, si bien en México existen las denuncias y los procesos judiciales, también existen en la aplicación de la ley amplias deficiencias y vicios que orillan a las personas a no utilizar estos mecanismos o herramientas procesales de defensa. Por poner un ejemplo: la ley parte de que cuándo no se opongan al tratamiento de datos incluido en el aviso de privacidad se dará por entendido el consentimiento en el tratamiento, a esto se le conoce como "consentimiento tácito" (Art. 8 de la LFPDPPP). Este ejemplo es importante por muchas razones: primero porque el aviso de privacidad suele ser un tratado y no un aviso, y luego porque si alguien se niega al tratamiento de sus datos el servicio que solicita no le es otorgado. Entonces la persona queda atrapada entre el tiempo, los procesos y los procedimientos burocráticos que tanto en las empresas como en las autoridades gubernamentales y/o del Estado deben realizar para cumplir y hacer cumplir sus derechos.

El asunto no termina ahí, el hecho de que este diseño quedara plasmado en el modelo de protección de datos personales se debe en gran parte a las pugnas del sector empresarial e industrial y al acuerdo de las autoridades en el Congreso de la Unión, a los representantes del IFAI y por supuesto algunos académicos y miembros de autoridades internacionales que así lo consensuaron. Al respecto hemos dicho que los aspectos más discutidos de la protección de datos personales fueron el consentimiento, las funciones del órgano garante, las sanciones y las multas. Aunque también estuvieron en el escenario de los acuerdos los criterios para el flujo trasfronterizo de datos y la definición de datos sensibles. A continuación, se identifican las consecuencias de cada uno de estos temas para la persona en lo particular.

El consentimiento es uno de los elementos más importantes de la protección de datos personales, porque a partir de allí se define o no el tratamiento de los datos. El consentimiento es

el acto; “la manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de estos datos” (Art. 3, Fracción IV de la LFPDPPP). El consentimiento puede ser tácito —como ya se ha descrito— o expreso… “será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos” (artículo 8 de la LFPDPPP). Este consentimiento expreso puede ser verbal o escrito. Es verbal cuando “se considera que el titular lo externa oralmente de manera presencial o mediante el uso de cualquier tecnología que permita la interlocución oral (art. 18 del Reglamento) y será “escrito cuando el titular lo externe mediante un documento con su firma autógrafa, huella dactilar o cualquier otro mecanismo autorizado por la normativa aplicable. Tratándose del entorno digital, podrán utilizarse firma electrónica o cualquier mecanismo o procedimiento que al efecto se establezca y permita identificar al titular y recabar su consentimiento” (Art. 19 de reglamento).

Entonces a partir del consentimiento se da el tratamiento de datos. De no manifestarse dicho consentimiento no hay acto jurídico y con ello consecuencias; pero si por algún motivo éste se manifiesta de cualquier manera considerada en la norma, traerá invariablemente alguna consecuencia, por ello los agentes en la participación en el diseño de las instituciones y de la autoridad para la protección de datos personales pugnaron por las características de este consentimiento. Sin duda es primordial que la persona conozca esta información, pues muchas veces da su consentimiento sin saberlo. En segundo lugar, la teoría del diseño institucional reconoce la necesidad de que las instituciones estén basadas en el contexto social al que hacen referencia y si se está partiendo de una sociedad como la mexicana donde 4.7 millones de personas de más de 15 años no saber leer ni escribir (INEGI, Encuesta Intercensal 2015), y que habría que agregar los casi 3 millones (también mayores de 15 años) que sólo cursaron los dos primeros años de la instrucción primaria. Se trata entonces de aproximadamente siete millones de mexicanos que, en realidad, son analfabetos, por lo tanto, si las personas necesitaran un servicio donde se da el consentimiento una vez mostrado el aviso de privacidad, la realidad es que siete millones de personas, por considerar sólo a los analfabetos, darían su consentimiento sin saber el motivo de éste (Narro y Moctezuma, 2012).

Bajo estas circunstancias se requiere un sistema de planeación nacional sustentada en las obligaciones jurídicas y morales de una protección basada en los valores democráticos. Es como dice Stefano Rodotá “una tutela efectiva de la privacidad se transforma, entonces, en elemento básico para que una ´sociedad´ pueda seguir llamándose ´democrática´. Donde la idea del ´hombre de vidrio´ se desecha totalmente cuando se habla de protección de datos personales en contextos

democráticos".

Ahora bien, las excepciones al consentimiento son dos: al tratamiento (Art. 10 de la LFPDPPP) y a la trasferencia nacional o internacional (Art. 37 de la LFPDPPP) en casos específicos, como por ejemplo para el tratamiento no se requiere consentimiento cuando sean fuentes de acceso público. Esto quiere decir que por ser una fuente de acceso público para tratar los datos no se requiere consentimiento y esta disposición es muy dispersa porque la definición de fuente de acceso público también lo es. Respecto a la transferencia internacional o nacional de los datos personales es preocupante la parte donde se dice que esta transferencia "es efectuada a sociedades controladas, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas interna", así mismo "cuando sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia". En este sentido la transferencia parte del supuesto de que existen medidas de seguridad razonables entre la entidad emisora y la receptora (responsable y encargado) de los datos personales, pero estas figuras complejizan el sistema y por lo tanto también la protección. Las transferencias de datos también deben tener un límite, aunque se prevé que tengan su límite en los principios de tratamiento, violaciones a la protección de datos personales y/o la privacidad de activistas sociales o periodistas, permiten argumentar la necesidad de que el uso o transferencia de datos personales, por ejemplo, tengan también un límite jurídico y administrativo.

Otra deficiencia que a la fecha no se soluciona es que para el sector público no se reconoce el derecho de cancelación y oposición. En este sentido es importante manifestar que en algunos casos es necesario y posible tener estos derechos y que por lo tanto deben estar contemplados en la ley, puesto que en la Constitución sí están previstos. Existe por lo tanto una insuficiencia en las leyes federales y locales que son aplicadas. Cuando las instituciones se crean es importante considerar las particularidades de los contextos. Estas particularidades no sólo son económicas, sino también sociales, políticas y hasta culturales. Lo que hasta este momento se alcanza a ver es que se contemplaron principalmente dos aspectos: el económico y el jurídico positivo.

El problema más grande al que se enfrenta la persona ante el diseño actual de protección de datos personales son los procesos administrativos y jurídicos para logar la protección de sus datos. Ante un robo de identidad internacional, por ejemplo, la legislación aplicable es diversa y requiere herramientas que provean protección sistemática y coherente, pues en "la transición de la *vieja a la nueva tecnología* los individuos *comunican cada vez más y dan cada vez más*

información el mundo ha de decir: *Yo soy la persona que puede controlar mi vida*. Y, además, debe respaldarse con una *protección pública de la privacidad y la protección ante la prepotencia del mercado. Las personas han de tener el derecho a no ser seguidos en su navegación por la Red. Google, Facebook, Apple… son mucho más poderosos que los individuos. Les dan servicio a cambio de que les den información. Por eso los poderes públicos han de dar protección a las personas*", incluso más allá de las propias personas. Hay que oponerse a ser perfilado por razones de mercado o por poderes políticos. Hay que "silenciar el chip" (Stefano Rodotà, 2012) y eso se logrará en la medida en que se acepte a la protección de datos personales como un problema público complejo, necesitado de soluciones coherentes, transversales, nacionales y aplicadas desde la protección máxima que tenemos: los poderes públicos.

5.2 Las consecuencias para el sector empresarial e industrial

En el Estado democrático de derecho no sólo se respetan las libertades individuales, la vida privada de las personas y los datos personales para dar pauta a la libre manifestación de la actuación humana en torno a su libertad, integridad y dignidad. También se respetan otros principios constitucionales como la libre profesión, la promoción de la economía, el libre mercado, la competitividad y la libertad empresarial, y más aun contemplando que el contexto económico hace referencia a una economía neoclásica de libre mercado. En esta economía las relaciones comerciales adquieren relevancia para el desarrollo y el crecimiento económicos, afectando invariablemente la relación con las personas y los Estados. El reconocimiento en un Estado democrático de la libertad económica implica que el Estado también la deba observar por respeto a este principio constitucional.

Antes de iniciar este análisis es importante aclarar y desmitificar la idea de que las empresas o las industrias son los enemigos a combatir. Existen varias definiciones de empresa, las más comunes dicen que es "una organización o institución dedicada a actividades o persecución de fines económicos o comerciales para satisfacer las necesidades de bienes o servicios de los demandantes, a la par de asegurar la continuidad de la estructura productivo-comercial, así como sus necesarias inversiones. En este sentido es una organización con fines lucrativos, pero también es una herramienta para proveer bienes y servicios. Desde un punto de vista más social "es un grupo social en el que, a través de la administración de sus recursos, del capital y del trabajo, se producen bienes o servicios tendientes a la satisfacción de las necesidades de una comunidad". Entonces se puede decir que la empresa si bien tiene como uno de sus principales fines obtener ganancias,

también existe la contraparte que es la provisión de bienes o servicios, y empleos. Sin dejar de considerar que también crean necesidades y abusan de sus insumos de producción.

En México el Artículo 25[48] de la Constitución define la economía como una economía mixta. Donde se reconoce la rectoría económica del Estado, pero también la participación de otros actores. Al respecto dice: "el Estado planeará, conducirá, coordinará y orientará la actividad económica nacional, y llevará al cabo la regulación y fomento de las actividades que demande el interés general en el marco de libertades que otorga esta Constitución". Asimismo "al desarrollo económico nacional concurrirán, con responsabilidad social, el sector público, el sector social y el sector privado, sin menoscabo de otras formas de actividad económica que contribuyan al desarrollo de la Nación". Estas características de la economía mexicana obligaron en parte, por ser garantías económicas a particulares, la necesidad de considerar las normas internacionales que les permiten convivir en un contexto internacional. De esta manera, como mencionamos en el capítulo anterior, se retomaron aspectos del modelo de protección *Safe Harbord*, del modelo garantista de la Unión Europea y del modelo del Foro Económico Asia Pacífico (APEC). Estas consideraciones dieron origen, en gran parte, al diseño institucional y organizacional de la protección de datos personales en México, principalmente en el ámbito del tratamiento de datos en posesión de los particulares.

Entender el modelo garantista implica reconocer la protección de la persona y el reconocimiento de la protección de datos como derecho humano fundamental, pues a partir de allí se pueden justificar los límites económicos a las empresas ajenas a la economía europea. Por lo tanto, también se debe observar el aspecto económico del modelo de protección de datos garantista. Este modelo, desde lo económico, puso límites a empresas estadounidenses como Google, Apple, Microsoft, HP, Dell e IBM. Son barreras al manejo de datos, barreras económicas argumentadas y fundadas en derechos humanos fundamentales. Por supuesto que no son barreras absolutas, pues existen herramientas de coordinación transfronteriza de datos personales entre ambas economías. Sin embargo, a partir de esta razón se puede entender, desde el punto de vista económico, a la protección de datos personales en el continente europeo.

[48] Corresponde al Estado la rectoría del desarrollo nacional para garantizar que éste sea integral y sustentable, que fortalezca la Soberanía de la Nación y su régimen democrático y que, mediante la competitividad, el fomento del crecimiento económico y el empleo y una más justa distribución del ingreso y la riqueza, permita el pleno ejercicio de la libertad y la dignidad de los individuos, grupos y clases sociales, cuya seguridad protege esta Constitución. La competitividad se entenderá como el conjunto de condiciones necesarias para generar un mayor crecimiento económico, promoviendo la inversión y la generación de empleo." Párrafo reformado DOF 28-06-1999, 05-06-2013, en: http://www.diputados.gob.mx/LeyesBiblio/htm/1.htm

El modelo sectorial o *Safe Harbord* de los Estados Unidos y Canadá[49] también influenció sensiblemente el diseño mexicano. Los sectores económicos pugnaron porque en México no se requiriera el permiso de la autoridad garante para realizar un flujo trasfronterizo de datos, asimismo porque el consentimiento se diera por sentado una vez mostrado el aviso de privacidad, aunque este aviso debe estar basado —según la norma— en los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad. Se pugnó porque existiera una autoridad garante, pero también otras autoridades regulativas, así como la exclusión de las sociedades de información crediticia y la continuidad de otras autoridades responsables, que coadyuvaran, en la protección de datos personales como la Procuraduría Federal del Consumidor o la Secretaría de Economía. Esto permitió a las empresas una cierta facilidad en las relaciones económicas relacionadas con protección de datos y la publicidad.

Con respecto a las sanciones y las multas, el monto acumulado de las multas por violaciones a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, en vigor desde enero de 2012, es de 100 millones 516,107 pesos, informó el IFAI, el cual indicó que el pleno del organismo ha resuelto 34 procesos de imposición de sanciones por incumplimientos al marco normativo. Ha detallado que las multas acumularon dos millones 45 pesos en 2012; 56 millones 662,740 pesos en 2013, y 41 millones 853,321 pesos en 2014. En 19 de los 34 casos se aplicaron sanciones económicas por contravenciones a los principios de la Ley, en cinco por incumplimiento del deber de confidencialidad, en cinco por cambiar de manera sustancial la finalidad original del tratamiento de los datos y en 14 por recabar o transferir datos sin consentimiento.

Lo anterior, luego de que impuso una multa a una empresa por violar la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, que ya se cubrió ante la Secretaría de Finanzas del Gobierno del Distrito Federal. En ese caso la empresa obtuvo datos personales de una de sus empleadas sin dar a conocer, mediante su aviso de privacidad, la existencia y características principales del tratamiento al que serían sometidos, lo que implicó que con su conducta incumpliera el principio de información establecido en la norma. Los comisionados resolvieron en sesión privada del pleno imponer una multa por 129,520 pesos como consecuencia de las irregularidades detectadas durante la visita de verificación del IFAI.

[49] Canadá está certificada con nivel adecuado de protección de datos personales por la Comunidad Europea. Para profundizar en el tema, consultar: Secretaría de Economía. 2013. *Estudio de autorregulación en materia de privacidad y protección de datos personales en el ámbito de las TI*. 5ª versión final. PROSOFT 2.0, CANIETI y SE.

La sanción se fijó en esa cantidad porque dejó de garantizar la privacidad y el derecho a la autodeterminación informativa de la titular. Ello, en virtud de que no proveyó los mecanismos para que ésta pudiera ejercer su derecho a limitar el uso o divulgación de sus datos y los medios para que pudiera ejercer sus derechos de acceso, rectificación, cancelación y oposición. Con el pago de la sanción la empresa sentó un precedente, al constituir el primer caso en el que, como consecuencia de violar la ley, una infractora cumple voluntariamente la sanción que se le impone.

Por lo tanto, el sector empresarial e industrial se encuentra entre la permisión del paraíso económico y la obligación limitativa de las responsabilidades normativas de la protección de datos personales. Es decir, el modelo de protección de datos personales genera un entorno positivo para la empresa en torno al manejo de datos personales, pero también los obliga a cumplir estándares internacionales y regulaciones específicas que de no cumplirse conllevan sanciones punitivas considerables.

5.3 Las nuevas relaciones y procesos gubernamentales

El IFAI es la autoridad garante de la protección de datos personales. Autoridad que mantiene una estrecha relación con otras instancias reguladoras como la Secretaría de Economía y "todas aquellas que en el ámbito de sus atribuciones en materia de protección de datos deban coadyuvar con el IFAI" (art. 40 de la LFPDPPP).

En las siguientes líneas se analizan los efectos en el ámbito gubernamental a partir del federalismo; la coordinación entre autoridades garantes y reguladoras; las características constitucionales de la autoridad garante, sus funciones, competencias y atribuciones. Todo en su contexto político, administrativo y económico.

El sistema federal y la protección de datos personales mexicano fue muy simple en sus orígenes. En el texto constitucional de 1917 la Federación sólo podía hacer lo que expresamente se le asignara, mientras que los estados todo aquello que no hubiere sido establecido en favor de ella. Este modelo estuvo en vigor hasta 1934, cuando a fin de implantar la educación socialista, se facultó al Congreso de la Unión para emitir las leyes en las que se determinaran las competencias de la Federación y de los estados. En 1976 volvió a alterarse el modelo original, esta vez para facultar al Congreso a expedir las leyes que permitieran la concurrencia entre federación, estados y municipios en materia de asentamientos humanos. A partir de ese momento, el sistema federal mexicano entró en constante proceso de transformación. Al Congreso se le han asignado materias

para regularlas en vía de concurrencia, pero también mediante la coordinación y, más recientemente, con base en leyes generales.

Repasando rápidamente la situación actual de nuestro sistema federal, por una parte, hay materias exclusivas de la Federación y propias de las entidades federativas y municipios. Adicionalmente están las llamadas concurrentes, donde la distribución de competencias entre Federación, entidades federativas, Distrito Federal y municipios, corresponde a un órgano federal (asentamientos humanos, protección al medio ambiente, deporte o pesca, por ejemplo). También las de coordinación, en las que la Federación prevé las bases para que esos mismos niveles de gobierno convengan el ejercicio de competencias propias (protección civil, turismo, seguridad o salud). Finalmente, están las competencias que se ejercen con base en lo previsto en las leyes generales emitidas por el Congreso (protección de datos, archivos, elecciones, secuestro o trata de personas, entre otras).

Es importante especificar que la protección de datos personales hasta este momento se encuentra como una competencia exclusivamente federal cuando se trata de la protección de datos personales en posesión de los particulares, pero cuando se trata de los datos en posesión del sector público se diversifica y es una competencia no exclusiva de la Federación, sino también de las entidades federativas, las cuales emiten los lineamientos para las competencias municipales en materia de datos personales. En octubre de 2014 el IFAI sometió al Congreso de la Unión una propuesta de Ley general de protección de datos personales, con el objetivo de dar coherencia a un derecho humano fundamental en relación con las competencias federales y de las entidades federativas, pero sobre todo para asegurar congruencia en las garantías, derechos, obligaciones, sanciones, principios, valores y procedimientos relacionados con la materia. La Ley General de Protección de Datos en posesión de los Sujetos Obligados se encuentra como propuesta de ley en el Congreso de la Unión.

El ministro José Ramón Cossío señala que la única manera de comprender que mucho de lo que en el país sucede, más allá de errores o corrupciones, se debe a que la manera de asignar competencias entre los órdenes normativos por sí misma genera confusión, parálisis e ineficiencias. Es decir, en la Federación existen relaciones normativas dispersas y fragmentadas, no hay una, sino muchas maneras de gestión y con particularidades propias. Uno es el modo de ordenar los servicios de salud, otro el medio ambiente, otro la cultura. En realidad, no contamos con un sistema federal, sino con diversas modalidades de éste. En la complejidad actual hay situaciones donde distintas autoridades hacen lo mismo, donde ninguna puede hacer algo esencial, o donde quien

debiera controlar o vigilar no cuenta con facultades para hacerlo.

Esta es justo la problemática que presenta la protección de datos personales en México, un sistema federal disperso, sectorizado, y difícil de conciliar en sus obligaciones y competencias. Algunas entidades tienen ley y algunas no, algunos otros aumentan los sujetos obligados y otros los disminuyen, y en definitiva la diferenciación y sectorización origina que algunos reconozcan más o menos derechos, procedimientos, principios y valores diferenciados en torno a un derecho humano fundamental. "El mantener un sistema federal tan abigarrado como el nuestro, lleno de peculiaridades y excepciones, tan diferenciado por materias y modos de operación, no parece coadyuvar en la solución de nuestros problemas. Más bien, parece que el mismo es la causa generadora de muchos de ellos. En la actual crisis de sociedad y Estado, es indispensable considerar integralmente a nuestro sistema federal. Mucho de lo mal que van las cosas en muchos aspectos, puede explicarse tanto por su pobreza conceptual y operativa" (Cossío, 2015). Esta situación en materia de protección de datos personales se pretende solucionar con tres rediseños que se han implementado en México: el IFAI como organismo autónomo; el IFAI como institución nacional y con las Leyes Generales tanto de Acceso a la Información como de Protección de Datos Personales. Pero más allá de eso es necesario contar con un sistema nacional de protección de datos personales, un sistema de colaboración pública, privada, social. Una política nacional coherente con políticas y programas específicos.

El IFAI requiere de un sistema de coordinación que contemple las autoridades de las entidades federativas y las autoridades reguladoras como la Secretaría de Economía u otras que en el ámbito de sus atribuciones protegen y regulan en materia de datos personales. Este modelo híbrido que tenemos es parte de "una autoridad garante del derecho cuando los datos están en posesión de los particulares, pero con una normativa mínima general aplicable a todo, con la posibilidad de que autoridades sectoriales pudieran establecer normas que fueran más allá de lo que se estableciere en el ámbito general para cuestiones particulares, por ejemplo, financiero, salubridad, etc." (Alfredo Reyes Krafft, entrevista personal, 4 de diciembre de 2014). Es un diseño permisivo por estar fragmentado y disperso tanto en sus normas como en cuanto a sus autoridades.

En general, en el derecho y en la práctica de la política comparados se observa que los órganos constitucionales autónomos se crean, principalmente, por las siguientes consideraciones: 1. Porque existe la necesidad de desarrollar funciones nuevas —normalmente más complejas— que el Estado no realizaba en tiempos pasados y que por sus características no pueden llevar a cabo los órganos incluidos en las tradicionales teorías de la división de poderes; y 2. los órganos

constitucionales autónomos pueden surgir por cuestiones coyunturales de un Estado, determinadas por necesidades particulares de la acción política (Caballero, Fix, López, *et al*., 2011). En este sentido el INAI como organismo constitucional autónomo viene a realizar funciones antes no previstas, especializadas y que no sólo competen a relaciones internas, sino a relaciones con el entorno internacional. De allí el impulso externo que el INAI ha recibido para ser hoy un organismo garante de los derechos.

Las consecuencias de que el IFAI sea autónomo implicaron un aumento en su presupuesto, en sus funciones, en su estructura burocrática, en su sistema de relaciones gubernamentales, en los procedimientos y en el sistema jurídico mexicano su participación como actores activos en los procesos de controversias constitucionales y acciones de inconstitucionalidad (Carbonell, *et al*, 2011). Dentro de las razones para que el IFAI fuera autónomo se consideraron: la propia evolución del IFAI, sus atribuciones, la relación con otras autoridades federales y con los órganos garantes en las entidades federativas.

También el rediseño del IFAI consideró esencialmente su integración, el proceso de nombramiento de comisionados, su duración y las garantías de los titulares. En esencia se mantuvo el diseño del IFAI, pero se modificaron aspectos sustanciales para salvaguardar independencia y autonomía de los comisionados, el ejercicio presupuestario, la estructura burocrática, las funciones; la capacidad constitucional, de protección y garantías para las relaciones con el sector público y privado. También se consideraron contrapesos de responsabilidad de los comisionados (Carbonell, *et al.*, 2011).

Las relaciones que se prevén con otras autoridades son de responsabilidad, rendición de cuentas, fiscalización, auditorías, de coordinación regulativa y de régimen interno. Las relaciones de responsabilidad y rendición de cuentas son con el poder Legislativo, previéndose informes anuales de las actividades. Desde el punto de vista interno, actualmente el órgano interno de control (OIC) es designado y depende de la Secretaría de la Función Pública (SFP) y los procedimientos disciplinarios son conocidos por éstos o bien por los órganos centrales. Su transformación en organismo constitucional autónomo modificará sus órganos de control y vigilancia.

El INAI como organismo autónomo se constituye como órgano especializado, capaz de resolver controversias en el acceso a la información pública y la protección de datos, con excepción de la competencia relativa de la Suprema Corte de Justicia de la Nación como tribunal constitucional y órgano límite del orden jurídico mexicano. Además de ser la principal institución en torno a la protección de datos personales capaz de coordinar y articular a las autoridades

federales y estatales en la materia. Esta coordinación deberá ser técnica, funcional, de principios, valores y hasta estructural. Por ejemplo, en materia de solicitudes de derecho para la protección de datos personales en las entidades federativas, donde el INAI habilitará el uso de una Firma Electrónica, para la presentación y sustanciación de las solicitudes de protección de derechos y de las denuncias por presuntos incumplimientos a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, promovidas al amparo del presente acuerdo en el sistema electrónico del Instituto. Para el caso de la presentación de denuncias en el sistema electrónico del Instituto también se admitirá la firma autógrafa.[50]

El IFAI pasó de ser un organismo dependiente de la Administración Pública para convertirse en constitucional y tener las facultades para "promover acciones de inconstitucionalidad, en contra de leyes de carácter federal, estatal y del Distrito Federal, así como de tratados internacionales de los que México sea parte, que vulneren el derecho a la protección de datos personales o el acceso a la información. De la misma forma se le dota de esta facultad para promover acciones de inconstitucionalidad a los organismos garantes de las diversas entidades federativas, en contra de las leyes expedidas por sus respectivas legislaturas locales, y en su caso, por la Asamblea Legislativa del Distrito Federal.

Se establece la procedencia de controversias constitucionales tratándose de conflictos competenciales entre dos órganos constitucionales autónomos, y entre uno de éstos y el Poder Ejecutivo de la Unión o el Congreso de la Unión sobre la constitucionalidad de sus actos o disposiciones generales. Se amplía el abanico de los sujetos obligados por la legislación en materia de transparencia y acceso a la información pública, siendo esto aplicable también a los responsables en materia de protección de datos personales. En consecuencia, los sujetos obligados por el artículo 6º constitucional se extienden a "los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona, física, moral o sindicatos, que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal; con excepción de aquellos asuntos jurisdiccionales que correspondan a la Suprema Corte de Justicia de la Nación, en cuyo caso resolverá un comité integrado por tres ministros." (Artículo 6º, apartado A, fracción VIII, párrafo cuarto de la

[50] Acuerdo por el que se establece el sistema electrónico para la presentación de solicitudes de protección de derechos y de denuncias, así como la sustanciación de los procedimientos previstos en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. http://inicio.ifai.org.mx/MarcoNormativoDocumentos/18.%20Acuerdo%20establece%20sistema%20electr%C3%B3nico%20%28DOF%2028-11-13%29.pdf

Constitución Política de los Estados Unidos Mexicanos.)

Se faculta al órgano constitucional autónomo de carácter nacional para conocer "de los recursos que interpongan los particulares respecto de las resoluciones de los organismos autónomos especializados de los estados y el Distrito Federal que determinen la reserva, confidencialidad, inexistencia o negativa de la información, en los términos que establezca la ley" (artículo 6º, apartado A, fracción VIII, párrafo cuarto de la Constitución). De este precepto constitucional se desprende que el recurso de revisión ante el órgano garante nacional respecto de las resoluciones emitidas por los demás organismos autónomos locales podría proceder tanto en materia de acceso a la información como en materia de protección de datos personales, no sólo porque introduce aquellas resoluciones relativas a la confidencialidad (siendo uno de los ejes rectores de la protección de datos personales), sino además porque el término "información" abarca tanto a la información pública gubernamental como a cualquier información concerniente a una persona física, identificada o identificable.

Se establece para el órgano constitucional autónomo de carácter nacional la facultad de atracción para conocer, "de oficio o a petición fundada del organismo garante equivalente del estado o del Distrito Federal" de los recursos de revisión que por su interés y trascendencia así lo ameriten (artículo 6º, aparado A, fracción VIII, párrafo quinto). Como puede observarse de este precepto, la facultad de atracción queda en términos muy abiertos, por lo que su alcance y configuración quedan sujetos a lo que disponga la ley reglamentaria.

De todo lo anterior podemos deducir que el órgano garante constitucional del derecho a la protección de datos personales se constituye en un 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. Este último aspecto se manifiesta tanto en las facultades que le otorga la Constitución para ejercer el recurso de revisión de las resoluciones de los organismos autónomos especializados de las entidades federativas, como en su facultad de atracción.

Precisamente esta segunda dimensión de las facultades del órgano constitucional autónomo es la que trae aparejada la necesidad de crear una Ley General cuyo objetivo, en términos de la propia Constitución, consiste en establecer "las bases, principios generales y procedimientos del ejercicio de este derecho, e implementar un piso mínimo que establezca la simetría en el ejercicio del derecho en cualquier orden de gobierno que garantice su plena efectividad.

En este capítulo analizamos causas y efectos del diseño —modelo— de protección de

datos personales en México. Logramos observar efectivamente que los intereses económicos tanto públicos como particulares promovieron una regulación descentralizada, dispersa, sectorial, para dar cabida a la libertad económica empresarial e industrial, pero que a la vez se originó un sistema de procesos y procedimientos confuso y hasta conflictivo entre la persona, el gobierno y las empresas. En la sección de Conclusiones se profundizará en los hallazgos.

CONCLUSIONES

"Una política prisionera de la tecnología puede dar la impresión de mayor eficiencia, pero hace más débil a la democracia"

Stefano Rodotà.

La protección de datos personales es un derecho autónomo diferente del derecho a la privacidad, a la intimidad y a la autodeterminación informativa. Todos estos derechos tienen una particularidad: están relacionados con la persona y con la libertad. El derecho a la protección de datos personales es un derecho autónomo, nuevo y de tercera generación. Es un derecho indirecto cuando se requiere hacerlo valer y garantizarlo para poder proteger otros derechos, por ejemplo: toda persona tiene derecho a ser protegida, por ejemplo, en sus datos de salud, y la protección de los datos de salud muchas veces se protegen para evitar alguna discriminación sobre alguna enfermedad en específico, entonces aquí el derecho a la protección de datos personales sirve para proteger otro derecho, que es —para este caso— el derecho a la no discriminación. Se protegen los datos personales de salud para evitar discriminación, y para este caso es un derecho indirecto.

También es un derecho directo personalísimo que implica la protección misma de la persona, a partir de la protección de los datos en sí. Estos casos suelen pasar en ejemplos de redes sociales, donde toda la información que le concierte o se relacione con la persona está protegida de manera directa, y al proteger la información en sí misma, se protege a la personalidad.

En este sentido se entiende porqué la protección de datos personales ha sido estudiada principalmente por el derecho y por las ciencias relacionadas con la tecnología y la computación. Sin embargo, este derecho ha evolucionado de tal manera que se requiere no sólo el reconocimiento constitucional, sino también leyes, reglamentos, lineamientos, códigos de conducta, procesos, procedimientos, autoridades garantes, autoridades de control, autoridades reguladoras y todo un conjunto amplio de planes y programas tanto en el sector privado como en el sector público, motivo por el cual la protección de datos personales también debe entenderse como una política nacional que incluya por supuesto políticas y programas específicos. Es decir, un derecho humano fundamental que requiere a la vez de una política coherente, sistematizada, coordinada y con objetivos claros.

La política de la información, como propuesta, pretende ser el timón gubernamental del manejo de la información por parte del Estado. El Estado como garante de la seguridad, la libertad y la propiedad, tal como es considerado el Estado democrático liberal de derecho. Este derecho no

puede ser enmarcado en el esquema de "ser dejado solo" porque las estructuras y mecanismos institucionales y organizacionales, tanto de las empresas como de los Estados, son comparativamente superiores a las de la persona en lo individual y particular. Hay sin duda una falta de equilibrio entre las herramientas de protección entre cada agente.

Entonces la protección de datos personales es un derecho humano fundamental en México. Es diferente a la intimidad y a la privacidad, aunque relacionado porque poseen principios superiores que los vinculan, como la libertad individual. Es un problema complejo y requiere la acción del Estado y del gobierno, pero una acción sistemática, coherente y transversal. Sistemática porque es un tema que trasciende territorios físicos y virtuales, coherente para facilitar la actuación de la persona frente a la seguridad y protección de sus propios datos, y transversal porque tanto el sector público como el privado manejan datos personales.

El tema de la protección de la persona tiene importancia cuando se aprecia desde la óptica de la democracia. A partir de ella se puede asegurar un espacio de libertad para ser y hacer, un espacio libre de interferencias totalitarias por parte del Estado y de las empresas privadas, que hoy también pueden vulnerar derechos. Una idea clara del significado de los datos personales para una nación es iniciar con la responsabilidad jurídica y moral que tiene el Estado. Es reconocer el problema como nacional y complejo, ante el cual el gobierno mediante una política pública específica no podrá atacar los diferentes frentes de la protección de datos personales. Debe ser más bien una política nacional. Esta política nacional es congruente con las estipulaciones jurídicas de los artículos 25, 26 y 28 de la Constitución, en la que se concibe aún al Estado como un eje fundamental en la planeación nacional, en la dirección del desarrollo nacional y en la competitividad. Estos artículos constitucionales permiten desde el punto de vista jurídico delinear una política nacional de la información, específicamente la de los datos personales.

Esta política pública de Estado incluye protección dentro y fuera del territorio, es por lo tanto un proceso sistemático. Esta política requiere una autoridad garante y la estructura funcional del INAI está acorde con las necesidades administrativas para la implementación de esta política, aunque las políticas específicas implicará relacionarse con otras áreas económicas, comerciales e industriales tanto nacionales como internacionales, de tal manera que se requerirá crear el Sistema Nacional de Datos Personales, donde la Ley General de Datos Personales en Posesión de los Sujetos Obligados puede ser la norma general que provea de principios, funciones y proceso a esta nueva política nacional.

En dicha Ley será necesario ampliar las posibilidades administrativas para la persona. Es

decir, un litigio penal o civil en México son extensos en tiempo y procedimientos, por lo tanto, debe ser el ámbito administrativo tanto público como privado el que provea de herramientas de protección a la persona para su seguridad y protección. Por ejemplo, una política específica deberá estar dirigida a proveer de herramientas técnicas de software computacional para que la propia persona pueda adquirir, instalar, administrar y actualizar su protección en el uso de bienes y servicios en la red virtual.

El resultado de esta propuesta podría parecer paradójico con respecto a las libertades económicas, pero al contrario, pues de implementar una política mucho más sistemática, las transacciones comerciales podrán realizarse con mayor seguridad de otros continentes a México. Es no sólo proteger el ámbito propio de estas libertades individuales, sino también velar por la libertad económica nacional. De este modo es posible concluir que el derecho fundamental a la protección de datos personales se transforma en un elemento básico de la nueva ciudadanía electrónica y las relaciones comerciales para la competitividad, la innovación y el desarrollo tecnológico. De aquí la necesidad de coincidir con algunos juristas como Stefano Rodotà que asegurar la necesidad de promulgar los derechos digitales del hombre, dentro de los cuales está la protección de sus datos.

Idear, planear y administrar la información digital de las personas en un país determinado implica reconocer las necesidades tecnológicas capaces de resolver problemas a partir de contexto políticos y económicos específicos. En este desarrollo tecnológico se deben contemplar las necesidades de bienes y servicios para la ciudadanía. Por ejemplo, en el caso de la recaudación fiscal, donde el gobierno puede aumentar sus niveles de recaudación al mantener de innovación tecnológica que además de seguridad, certidumbre, información, agilidad y sensatez, puedan aumentar la confianza para cumplir con las obligaciones de las contribuciones a la cuenta pública. De allí que en esta investigación se haya analizado el caso de la *e.firma* en el Servicio de Administración Tributaria.

Entonces, de las conclusiones se tiene que la protección de datos personales, como se ha demostrado en esta investigación, es un tema eminentemente económico, por supuesto que se vieron involucrados los intereses políticos y en cierta medida los sociales, pero con una tendencia económica que inclinó los diseños institucionales. De allí la importancia de enmarcarlo en la discusión de la democracia, la ciudadanía, los derechos y el reconocimiento de la dignidad, seguridad y vida de la persona en la era digital. Pero también como un medio de innovación, desarrollo y competitividad, principios preponderantes en la toma de decisiones para el diseño

institucional y organizacional de la protección de datos personales en México.

México es un modelo híbrido de protección de datos personales, modelo influenciado por la Comunidad Europea, pero también por el modelo de Estados Unidos de América. La primera iniciativa de protección de datos personales presentada por el exsenador Antonio García Torres en realidad era una propuesta tendiente a la protección exhaustiva de la persona y de su información, fue detenida porque el sector industrial en representación de asociaciones como AMIPCI, ABM y ANTAD negociaron en el Congreso de la Unión primero la salida de Ley de Acceso a la Información, quien junto con miembros de la academia lograron promover y dejaron la protección de datos personales como un tema sólo para el sector público, con una deficiente regulación que tuvo la necesidad de ampliarse con lineamientos débiles en su diseño y aplicación.

De allí se constituyó la idea de que el IFAI era también el garante de la protección de datos personales en el ámbito del sector público, lo cual si bien fue cierto, la realidad es que sólo era una autoridad del acceso a la información, pues así se constituyeron y se formaron una reputación en ese ámbito, y la protección de datos personales sólo tomo fuerza, auge e importancia cuando el senador Antonio García Torres y otros legisladores insistieron en proponer una ley específica en la materia, así como la creación de una autoridad distinta al IFAI para garantizarlo.

Las iniciativas en su generalidad proponían una autoridad diferente y leyes especializadas en la materia, pero fue nuevamente el sector privado quien de manera legítima tomó parte en la discusión, el diseño y las decisiones finales del modelo de protección de datos personales en México. Estudios, datos, negociaciones y propuestas encontradas dieron la luz a un modelo que retoma al consentimiento como el núcleo duro de la protección de datos personales. Se logró constitucionalizar la protección de datos personales como derecho humano fundamental y una garantía de esta protección, pero también se flexibilizó el consentimiento. Fue sin duda una negociación económica y política que tuvo beneficios, pero también perjuicios tanto para el gobierno, como para las empresas y por supuesto para el individuo, que resultó ser el más afectado. Toda acción tiene consecuencias y para el individuo fue el más afectado en este diseño.

Por lo tanto, la política de protección de datos personales deberá estar basada en principios democráticos que permita su protección amplia y sustantiva, y deberá ser eficiente, capaz de incluir la participación de las personas en el diseño e implementación de la política, con el objetivo de tener control de los datos. Se debe ir más allá de prometer eficiencia administrativa y el ocultamiento de los intereses sobre el tratamiento de los datos. Se trata de diseños basados en la información, la persona y con la capacidad de poder implementarse sin dejar vulnerable a los

individuos frente a los corporativos o los gobiernos, que a partir del discurso de la seguridad y la eficiencia perjudican la personalidad de los seres humanos, sin convertirlos sólo en insumos del mercado o del Estado. Es decir, con capacidad de acción y decisión. De libertad, inclusión, decisión y acción.

Esto lo podemos corroborar ante la ilegalidad en la recolección de los datos por parte del Servicio de Administración Tributaria para la *e.firma*. Caso que carece además de un sistema claro de información al ciudadano, al contribuyente. Pero que también es violatorio del principio que rige a la Administración Pública, el de competencia. Pues la dependencia facultada para realizar esa recolección es la Secretaría de Gobernación y esta recolección para la cédula de identidad fue detenida por no cumplir con los aspectos normativos de la privacidad y la protección de datos, según las evaluaciones de impacto a la privacidad realizadas por el Dr. José Luis Piñar.

El caso de la *e.firma*, muestra la complejidad del problema, pero también muestra que el INAI se ve rebasado por la cantidad de situaciones particulares que se presentan día a día y que por ser tan complejo no alcanza a detectar. Al tener dos funciones, se concentra más en la de Acceso a la Información que en la de Protección de Datos. Siendo más bien pasiva, que activa, pues sólo actúa a petición de parte. De allí la necesidad de implementar políticas específicas sobre protección de datos personales con una autoridad activa, más que pasiva.

Aquí resulta de gran importancia detenerse un poco para referir los nuevos avances en la materia en México y el Mundo, siendo tres los principales: la promulgación del Reglamento Europeo de Protección de Datos Personales, el cual deja sin efectos la Directiva 95 del Consejo Europeo, la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, y el diseño de la Política Nacional de Protección de Datos Personales (PRONADATOS), dada a conocer en enero de 2018.

Si bien estas acciones podrían considerarse como un avance importante sobre protección de datos personales e incluso se podría decir que deja sin efectos algunos análisis realizados en esta investigación o dar por atendidas algunas de las recomendaciones realizadas, la realidad es que ni la ley, ni la política han sido suficientes para contener aún las consecuencias definidas por esta investigación en el último capítulo. El ciudadano sigue siendo el más afectado y los esquemas de protección poco han avanzado. Se le ha puesto mucha atención a la portabilidad de datos y se tiene al ciudadano con la feliz idea de portar sus datos de compañía a compañía, sin tener esquemas claros en el tratamiento de sus datos. Sobre estas acciones se podrían hacer varias referencias y análisis, sin embargo, no es el fin de esta investigación. Se mencionan justo por formar parte de

las acciones posteriores al análisis realizado en esta tesis, para conocer si de alguna manera afectan los resultados. Por el contrario, refuerzan la investigación y sus conclusiones, por mostrar la necesidad de una política nacional, la deficiente normativa para el sector público y porque han reforzado el papel de la economía y el mercado en materia de datos personales, dejando a la persona con mayores esquemas internacionales de vulnerabilidad.

En este sentido, el caso del SAT y las funciones rebasadas del INAI se pueden enmarcar en la categoría del gobierno digital y por ende de la democracia digital. En todos los espacios debe proveerse de herramientas de protección a la persona, porque como se demostró la política de protección de datos no se encarga de proteger a quienes no lo necesitan, sino de proteger a los más vulnerables en un contexto democrático. De proteger la libertad, los derechos, pero también derechos como la economía y el desarrollo tecnológico. Se requiere un sistema de privacidad como el creado para la expresión del voto en las elecciones. El anonimato como condición imprescindible para la libertad de expresión y la participación política. De ahí la necesidad de las evaluaciones de impacto a la privacidad como herramientas necesarias e imprescindibles para evaluar políticas antes de ser implementadas. La privacidad por diseño y por defecto. Todas estas son herramientas que poco a poco nos permitirán ir atacando los espacios discrecionales de la protección de datos personales.

Sin duda no existen derechos absolutos, pues todo derecho requiere una ponderación. Este punto es importante, pues la ponderación de derecho, principalmente entre el de acceso a la información y el de la privacidad es parte de lo que debemos discutir. No hay ponderación correcta, buena o mejor. Hay ponderaciones que pueden hacer alusión a principios, valores y conductas más o menos generales, aceptados por los ciudadanos de una nación. De allí la importancia de los acuerdos en el diseño institucional. De la participación e inclusión, herramientas con las cuales se tiene que definir la política.

Con el análisis del caso de la *e.firma* se logró identificar que los efectos para el gobierno son la falta de coordinación y entendimiento de la norma de protección de datos. Para el sector privado, los límites al desarrollo y a la cooperación económica nacional e internacional, así como las afectaciones para los empresarios más pequeños pues al tener que cumplir con las normas suelen afectar su competitividad. Finalmente, para las personas en lo particular se quedan sin opciones de protección ante un sistema que se judicializa, se amplía en tiempos y que logra más que beneficios personales, perjuicios, desinformación, manejo discrecional y complicado de los datos personales, vulnerando su derecho y todos los principios contemplados no sólo por la

legislación nacional, sino también por la internacional.

El principio italiano que dice “no pondremos la mano sobre ti”, es justo donde se debería fundar la nueva política de protección de datos personales, donde se respete el cuerpo de manera integral. Esta promesa de libertad que define al Estado Liberal de Derecho deberá estar por encima de los avances tecnológicos y los derechos económicos en el tratamiento de datos personales. De esta manera, cualquier tratamiento de datos biométricos ha de ser juzgado en referencia al cuerpo entero, a una persona que tiene que ser respetada en su integridad física y psíquica. Para crear un diseño institucional y organizacional capaz de comprender e interiorizar este principio. El principio *pro* persona, tal como lo llamamos en la legislación mexicana. Pero no sólo aplicado a la parte jurídica, sino a la administrativa también. Se trata de proteger a la persona en su integridad a partir de sus datos.

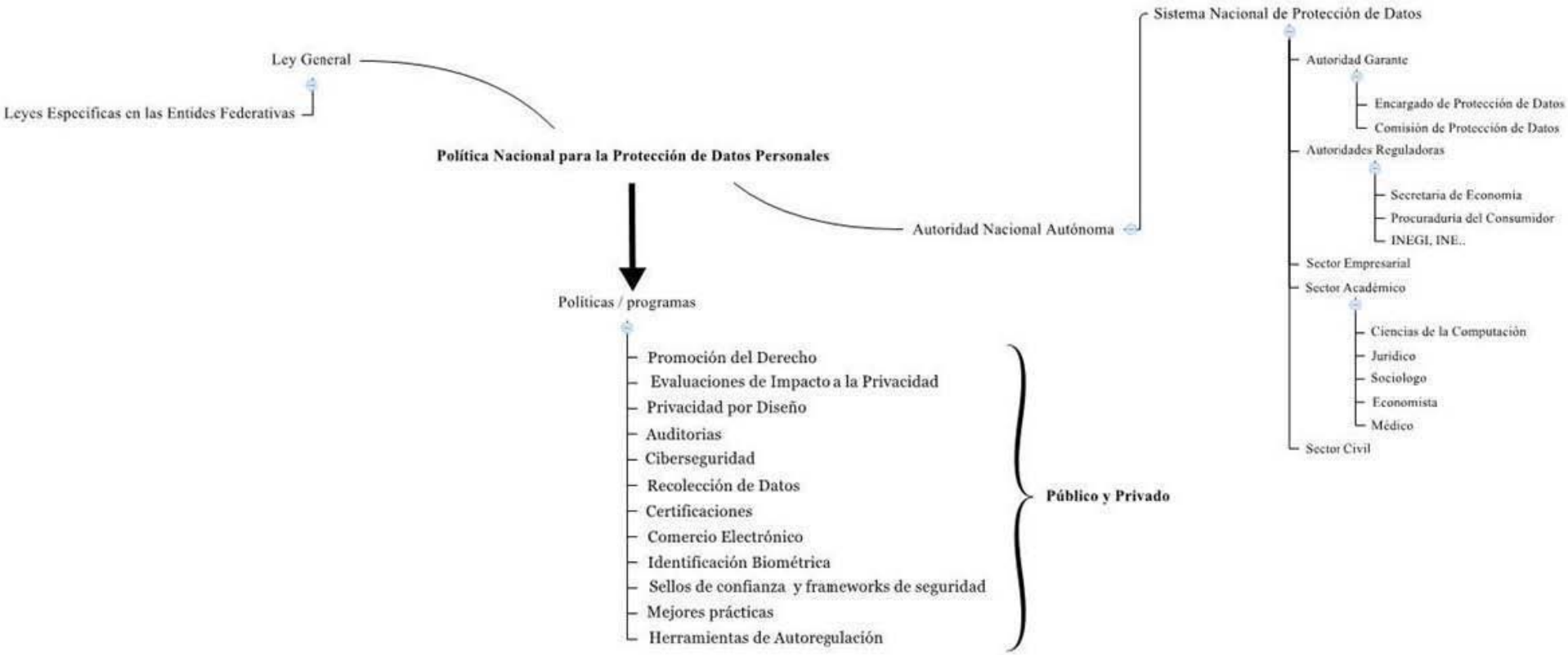
Una protección sistemática, coherente y transversal que sólo se logrará mediante una política nacional basada en principios reconocidos por los Estados nacionales. Esta política es una actuación frente a los contextos interno y externo. Esta política no limita el uso de la información bajo el consentimiento informado del tratamiento de datos, pero sí genera herramientas cercanas al ciudadano para su seguridad y protección. El diseño actual, por el contrario, expande la libertad económica y comercial, pero limita los derechos y la protección individual de la persona. Aquí corroboramos nuestra tesis de investigación.

La fragmentación normativa, la descentralización de las autoridades garantes y reguladoras, y la dispersión de la protección juegan un papel específico en el diseño de protección de datos personales. La fragmentación normativa permite reconoce la complejidad jurisdiccional de la regulación en materia de datos personales. Es decir, reconoce las tradiciones jurídicas nacionales. Un diseño no parte de cero, el diseño institucional tiene una base y la base para una nueva norma la constituyen tanto las formalidades como las informalidades en los procesos de toma de decisiones. Racionalidad y subjetividad de los actores en el diseño. Entonces el problema se debe a que los diseños normativos no parten de cero porque existen fórmulas nacionales o internacionales que los impulsan. Sin embargo, los problemas que tratan de resolver sí tienen una evidencia eminentemente empírica. De allí que los problemas de la realidad sobrepasan en mucho a las normas jurídicas y más aún cuando éstas no son flexibles, como en el caso del sistema jurídico mexicano.

La descentralización institucional y organizacional se visualiza desde dos aspectos. El primero obedece a la descentralización de los mecanismos de protección: protección de los datos

en posesión de los particulares y protección de los datos en posesión del sector público; protección nacional e internacional, territorial y extraterritorial. Y la segunda a la posición de las autoridades garantes y reguladoras, una autónoma y otras pertenecientes a la administración centralizada, en el caso de México. La dispersión hace referencia al tipo de datos que se desea proteger. Es decir, si es un dato médico, laboral, educativo, sentimental, político o sexual. En fin, cada tipo de dato tiene su propia regulación y esta situación complica las posibilidades de que la persona pueda tener control sobre su propia información. En el siguiente mapa se muestran los principales elementos de lo que aquí se considera como la política nacional de la protección de datos personales

Mapa 2. Diseño de la Política para la Protección de Datos Personales en México.



Fuente: Elaboración propia.

El diseño institucional de la Autoridad garante el México es el INAI, que para 2011 era una de las autoridades garantes con mayor tamaño a nivel internacional tanto en su estructura funcional, como en sus recursos. Hoy se constituye también como una autoridad con mayor cantidad de comisionados. En general el INAI posee en relación con las autoridades internacionales una posición privilegiada, de allí la necesidad de que en términos de datos personales genere resultados positivos en sus funciones y competencias.

En México el modelo de protección de datos personales tiene muchos retos, todavía la protección física y electrónica queda cuestionada ante la dispersión en las formas de vigilancia generales, de la conservación de datos de tráfico telefónico y en la red, de las tecnologías de localización, del cómputo en la nube y del uso de datos biométricos tanto en el sector público o privado. Por esto, frente al valor propio de la técnica necesitamos una reflexión continua sobre los valores básicos de la democracia, para distinguir entre los muchos usos de la tecnología democráticamente admisibles y los que no lo son, tal como lo refiere Stefano Rodotà "una política prisionera de la tecnología puede dar la impresión de mayor eficiencia, pero hace más débil la democracia". De aquí la importancia de que el gobierno promueva políticas sistemáticas, coherentes y transversales sobre la información: su acceso y protección. Una política con dos grandes brazos, siendo uno de ellos la política de protección de datos personales, con un conjunto amplio de herramientas, planes, programas, procesos claros, procedimientos, modelos de participación sociale incluso, muy importante, la promoción de este derecho como conocimiento colectivo, porque sólo de esta manera se logrará que la tecnología esté al servicio de las personas y no que la persona esté al servicio de la tecnología y del interés económico global.

FUENTES DE CONSULTA

Adinolfi, Giulio. 2007. A*utodeterminación Informativa, consideraciones acerca del principio general y un derecho fundamental.* Cuestiones Constitucionales, no. 17. Julio-diciembre 2007. México. Consultado en octubre del 2012 en: http://www.ejournal.unam.mx/cuc/cconst17/CUC000001701.pdf

Aguilar, Luis Felipe. 2010. *Política Pública.* Mèxico. Siglo XXI Editores.

Amerena, Eduardo. 2010. En Cámara de Diputados, 2010. *Retos y perspectivas legales en materia de protección de datos personales.* Convocado por la Comisión de Gobernación de la Honorable Cámara de Diputados, LXI Legislatura. Disponible en: http://www3.diputados.gob.mx/camara/001_diputados/010_comisioneslxi/001_ordinarias/020_gobernacion/013_ley_federal_proteccion_datos_personales/00001_discursos

Aragón, Sheyla. 2006. Iniciativa con proyecto de decreto para expedir la ley Federal de Protección de Datos Personales. Disponible en: http://sil.gobernacion.gob.mx/Archivos/Documentos/2006/03/asun_2235025_20060322_1143058385.pdf

Arellano David y Blanco Felipe. 2016. *Polìticas públicas y Democracia.* Cuadernos de divulgación de la Cultura Democrática. Mèxico. INE.

Arellano Gaul, David, 2000. *Reformando al gobierno: una visión organizacional del cambio gubernamental*. Mèxico. Centro de Investigación y Docencia Económicas (CIDE).

Arellano y Ochoa. 2012. Derechos de privacidad e información en la sociedad de la información y en el entorno TIC. Rev. IUS vol.7 no.31 Puebla ene./jun. 2013 Mèxico.

Arellano, David. 2010. El enfoque organizacional en la política y la gestión públicas. En Merino M. y Cejudo G. 2010. *Problemas, decisiones y soluciones. Enfoques de política pública.* Mèxico. Fondo de Cultura Económica. Pág. 61 – 92.

Arenas, Mónica. 2008. *La protección de datos personales en los países de la Unión Europea,* en Revista jurídica de Castilla y León, Nº. 16, 2008. España. Pág. 113 – 168.

Arendt, Hannah. 1958. *The Human Condition.* USA. University of Chicago Press

Banks, Jeffrey S. y Hanushek, Eric A. (eds.) (1995): Modern Political Economy. Old topics, new directions. USA. Cambridge University Press.

Baquero, María Eva. 2013. *The activity of the censors in the Administration of the Roman Republic.* Disponible el 5 de octubre de 2016 en

www.iustel.com/v2/revistas/detalle_revista.asp?id_noticia=412967.

Bauman, Zygmund. 1999. *La sociedad liquida.* España. Fondo de Cultura Económica.

Bennett, Colin y Charles D. Raab. 2003. *The Governance of Privacy. Policy Instruments in Global Perspectiva*. Gran Bretaña, Ashgate Publishing Limited.

Bennett, Colin J. 1992. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States.* Gran Bretaña. Cornell University Press.

Bennett, Colin. 2002. *Information Policy and Information Privacy: International Arenas of Governance.* Canadá. University of Victoria. Department of Political Science. Paper prepared for Journal of Law, Technology and Policy.

Berger y Luckmann. 1966. *La construcción social de la realidad.* USA. Penguin Random House.

Berlin, Isaiah. 1969 [1958]. *Four Essays on Liberty*. Oxford. Clarendon Press.

Black, Edwin. 2001. *IBM y el Holocausto. La alianza estratégica entre la Alemania nazi y la más poderosa de las corporaciones norteamericanas.* Buenos Aires. Atlántida.

Bobrow D. y Dryzek J. 1987. *Policy -analysis.* USA. University of Pittsburgh.

Caballero, Carbonell, Fix Fierro, López Ayllon, Roldán y Salazar. 2011. *El futuro del IFAI: consideraciones sobre su autonomía constitucional*. Mèxico. Centro de Investigación y Docencia Económicas (CIDE) y del Instituto de Investigaciones Jurídicas de la UNAM (IIJ-UNAM). Disponible en: http://biblio.juridicas.unam.mx/libros/7/3196/2.pdf

Cámara de Diputados. 2010. *Audiencias públicas con el Consejo Coordinador Empresarial.* Comisión de gobernación, LXI legislatura, 03 de marzo de 2010. Disponible en: http://www3.diputados.gob.mx/camara/001_diputados/010_comisioneslxi/001_ordinarias/020_gobernacion/013_ley_federal_proteccion_datos_personales/00005_audiencias_publicas

Cámara de Diputados. 2010. *Ley General de Protección de Datos Personales en Posesión de los Particulares.* Mèxico. Disponible en http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Cámara de Diputados. 2010. *Retos y perspectivas legales en materia de protección de datos personales.* Convocado por la Comisión de Gobernación de la Honorable Cámara de Diputados, LXI Legislatura. Disponible en: http://www3.diputados.gob.mx/camara/001_diputados/010_comisioneslxi/001_ordinarias/020_gobernacion/013_ley_federal_proteccion_datos_personales/00001_discursos

Cámara de Diputados. 2011. *Ley de Firma Electrónica Avanzada.* Mèxico.

Cámara de Diputados. 2016. *Código Fiscal de la Federación*, articulo 27. Mèxico. Disponible en http://www.diputados.gob.mx

Cámara de Diputados. 2016. *Constitución Política de los Estados Unidos Mexicanos*, articulo 27 Fracc. IV. México. Disponible en: http://www.diputados.gob.mx

Cámara de Diputados. 2019. *Constitución política de los Estados Unidos Mexicanos.* Mèxico. Disponible en: http://www.diputados.gob.mx

Cañas, Pedro. 2005. *Aspectos jurídicos del censo romano*. Boletín de la Facultad de Derecho, núm. 26. Mèxico. Instituto de Investigaciones Jurídicas. Consultado el 5 de octubre de 2016. Disponible en: http://espacio.uned.es/fez/eserv.php?pid=bibliuned:BFD-2005-26-58994FF6&dsID=PDF.

Carbonell, Miguel. 2004. *Los derechos fundamentales en México*. México. Comisión Nacional de los Derechos Humanos (CNDH) e Instituto de Investigaciones Jurídicas de la UNAM (IIJ-UNAM).

Carpizo, Jorge. 2009. *El sistema nacional no-jurisdiccional de defensa de los derechos humanos en México: algunas preocupaciones.* Anuario de Derechos Humanos. Mèxico. Nueva Época. Vol. 10. 2009, pp. 83-129. Disponible en: file:///C:/Users/Usuario/Downloads/21525-21544-1-PB.PDF

Cerda Silva, Alberto. Autodeterminación informativa y leyes sobre protección de datos. Revista Chilena de Derecho informático. No. 3 diciembre 2003 Pág. 47-75. Disponible en: http://web.uchile.cl/vignette/derechoinformatico/CDA/der_informatico_completo/0,1492, SCID%253D14331%2526ISID%253D507,00.html

Christensen y Laegreid. 2007. *Reformas post nueva gestión pública*. *Tendencias empíricas y retos académicos.* Revista Gestión y Política, Volumen XVI No. 2. Mèxico. Centro de Investigación y Docencia Económicas (CIDE). Pág. 539 – 564.

Christensen, Tom and Laegreid, Pierre. 2007. *The Whole-of-Government Approach to Public Sector Reform.* Public Administration Review, 67: 1059-1066. doi:10.1111/j.1540-6210.2007.00797.x

Cienfuegos Salgado, David. 2011. *El habeas corpus en México. Cuatro regulaciones en el ámbito local: Aguascalientes, Colima, Guerrero y Puebla.* México. Cámara de Diputados. Disponible en línea: http://www.diputados.gob.mx/sedia/sia/redipal/CRV-IV-ESP-04-11.pdf

Comisión Federal de Mejora Regulatoria. 2012. *Fortaleza institucional de las agencias*

reguladoras en México. Documento de Investigación en Regulación Núm. 2012-03. Noviembre del 2012. Disponible en: http://www.cre.gob.mx/documento/ReguladoresSociales.pdf

Consejo de Europa. 1968. *Recommendation 509. Human rights and modern scientific and technological Developments*. Disponible en: http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta68/EREC509.htm#1

Constant, Benjamín. 1989. *Escritos Políticos.* España. Centro de Estudios Constitucionales

Cornell University Law School. 2016 [1996]. Legal Information Institute. U.S. Constitution. Disponible en: Search Cornell https://www.law.cornell.edu/constitution/overview

Cossío Díaz, José Ramón. 2015. *Nuestro pobre federalismo. Hechos y Derecho.* Revista electrónica de opinión académica. Mèxico. El País, 11 de febrero del 2015.

Dahl, Robert A. 1971. *Polyarchy: Participation and Opposition.* USA. Yale University Press.

De León, P. 1977. Una revisión del proceso de las políticas: De Laswell a Sabatier. Gestión y Política Pública. 1. Mèxico. CIDE.

Del Castillo Vázquez, Isabel-Cecilia. 2007. *Protección de Datos: cuestiones constitucionales y administrativas. Derecho a saber y la obligación a callar.* España. Thomson Civitas y Agencia de Protección de Datos de la Comunidad de Madrid.

Deutsch, Karl W. 1971. *Los Nervios del Gobierno: modelos de comunicación y control político.* Argentina. Paidós.

Dryzek, John. 1990. *Discursive Democracy: Politics, Policy, and Political Science.* USA. Cambridge University Press.

EE.UU. Constitución. 1971. IV Enmienda. Bill of Rights.

EE.UU. Constitución. 1971. XVI Enmienda. Bill of Rights.

Elster, Jon. 1979. *Ulises y las sirenas: estudios sobre la racionalidad e irracionalidad.* USA. Cambridge University Press.

Federal Trade Comission. 2000. file:///C:/Users/ssalg/Downloads/United%20States.%20Federal%20Trade%20Commission%20-%20The%20real%20estate%20marketplace%20glossary%20_%20how%20to%20talk%20the%20talk-Federal%20Trade%20Commission%20(2008).pdf

Fernández, María. 2015. Marco jurídico estructural de la Administración Pública Federal. Mèxico, INAP.

Ferragoli, Luigi. 2006. *Sobre los derechos fundamentales.* Traducción de Miguel Carbonell. Mèxico. UNAM Consultado el 9 de octubre de 2012. Disponible en: http://www.ejournal.unam.mx/cuc/cconst15/CUC1505.pdf

Fountain, Jane E. 2013. *La construcción del Estado virtual.* Mèxico. Centro de Investigación y Docencia Económicas.

Galván Barceló, Juan Carlos. 2010. *Lopd, Safe Harbor: ¿golpe de timón del derecho anglosajón?* España. Disponible en: http://www.actualidadlopd.com/2010/10/06/lopd-safe-harbor-%C2%BFgolpe-de-timon-delderecho-anglosajon/

García González, Aristeo. 2007. *Nuevas tecnologías, un nuevo derecho: su reconocimiento en la norma Constitucional. Un estudio comparado.* Mèxico. Disponible en: http://www.themis.umich.mx/revistaDBN/pluginfile.php/80/mod_resource/content/0/NuevasTecnologias.

García Torres, Antonio. 2006. Minuta presentada para proponer en 2006 la propuesta de ley sobre protección de datos personales. Disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/iberoamerica/proyectos/common/pdfs/Proyecto-mexicano.pdf

Garfinkel, Simson. 2000. *Database Nation: The Death of Privacy in the 21st Century.* USA. O'Reilly Media, Inc.

Glancy, Dorothy J. 1979. *The Invention of the Right to Privacy.* Santa Clara University School of Law. USA. Arizona Law Review. Volumen 21, 1979. Número 1. Pág. 1 - 39. Disponible en línea: http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1318&context=facpubs

Glancy, Dorothy J. 1979. *The Invention of the Right to Privacy*. Santa Clara University School of Law, Arizona Law Review. Volume 21, 1979. Number 1. Disponible en línea: http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1318&context=facpubs

Goodin, Roberth E. 1996. *La teoría del diseño institucional.* USA. Cambridge, Cambridge University Press.

Gregorio G, Carlos. 2006. *Protección de datos personales: Europa vs. Estados Unidos, todo un dilema para América Latina.* México, Instituto de Investigaciones Jurídicas, UNAM.

Gregorio, Carlos G. 2006. *Protección de datos personales: Europa vs. Estados Unidos, todo un dilema para América Latina*. En Concha, Cantú, Hugo, Sergio López Ayllón y Lucy Tacher Epelstein (eds.). Transparentar al Estado: la experiencia mexicana de acceso a la

información. México, Instituto de Investigaciones Jurídicas, UNAM. Pág. 299 – 325.

Guerra Ford, Oscar G. 29 de enero de 2014. La protección de los datos personales en posesión del sector público y privado. InfoDF

Guerrero, Omar. 1986. *La teoría de la Administración Pública.* Mèxico. Harper and Row Latinoamericana.

Guichot, Emilio. 2007. *Acceso a la información en poder de la Administración y protección de datos personales.* En Revista de Administración Pública. 407 – 445. España. Centro de Estudios Políticos y Constitucionales.

Harold Lasswell. 1952. *The Policy Orientation, The Policy Sciences.* USA. Stanford University Press, pp. 3-15.

Hart, H.L.A. 1961. *El concepto de Derecho.* USA. Abeledo-Perrot.

Harvey, David. 2005. *A Brief History of Neoliberalism.* USA. Oxford University Press.

Hesse, Konrad. 1996. *Significados de los derechos fundamentales.* En Brenda y otros. Manual de derecho constitucional. Madrid. IVAP-Marcial Pons.

Huber, Rudolf. 2007. *Reforma de medios electrónicos ¿avances o retrocesos?* Mèxico. UNAM – Fundación Konrad Adenauer.

Igo, Sarah E. 2018. The Known Citizen. A History of Privacy in Modern America. Harvard University Press. Cambridge, Massachusetts. London, England.

Instituto de Investigaciones Jurídicas. 2011. Constitución Política de los Estados Unidos Mexicanos. México. IIJ-UNAM. Disponible en disponible en: http://info4.juridicas.unam.mx/ijure/fed/9/17.htm?s=

Instituto de Transparencia e Información Pública de Jalisco. 2010. Consideraciones sobre Habeas Data y su regulación en distintos ámbitos. Dirección Jurídica y de Capacitación. México. Disponible en línea: http://www.itei.org.mx/v3/documentos/estudios/estudio_habeas_data_6abr10.pdf

Instituto Federal de Acceso a la Información Pública. 2005. *5° Informe de labores.* Mèxico.

Instituto Federal de Acceso a la Información y Protección de Datos Personales. 2009. *Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales emitidas por el IFAI*. Mèxico. Disponibles en http://www.ifai.org.mx/datos_personales/seguridad/Recomendaciones_SDP.pdf, a 20 de agosto de 2009

Instituto Federal de Acceso a la Información. 2004. *Primer Informe de Labores.* México, Instituto

Federal de Acceso a la Información. Página 22.

Instituto Nacional de Estadística y Geografía. 2010. *Censo de Población y Vivienda 2010.* Mèxico.

Instituto Nacional de Estadística y Geografía. 2012. *Informe de actividades y resultados INEGI.* Mèxico.

Instituto Nacional de Estadística y Geografía. 2015. *Encuesta intercensal de 2015.* Mèxico.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. 2009. *Ley de Transparencia y Acceso a la Información Pública Gubernamental.* Mèxico. Disponible en: http://www.inai.org.mx/

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. 2005. *Lineamientos de protección de datos personales.* Publicados en el Diario Oficial de la Federación el 30 de septiembre de 2005. Disponibles en: Disponible en http://www.inai.org.mx/

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. 2016. *Lineamientos Generales de Protección de Datos Personales para el Sector Publico.* Publicados en el Diario Oficial de la Federación el 26 de Enero de 2018. Disponible en http://inai.org.mx

Instituto Nacional Electoral. 2016. *Distribución de ciudadanos en padrón de electores y lista nominal.* Mèxico. Disponible en: http://listanominal.ife.org.mx/ubicamodulo/PHP/index.php.

Jacint Jordana, David Levi-Faur y Xavier Fernández I. Marín. 2011. *The Global Diffusion of Regulatory Agencies: Channels of Transfer and Stages of Diffusion (2011). Comparative Political Studies* 1343. España. Instituto Barcelona de Estudios Internacionales (IBEI). Pag. 1343–1369.

Joskow, P.L. 2004. New Institutional Economics: A Report Card. USA. Massachussets Institute of Technology.

Kelsen, Hans. 1960. *Reine Rechtslehre: Mit einem Anhang: Das Problem der Gerechtigkeit.* Viena. F. Deuticke.

Kobrin, S. 2004. Safe harbours are hard to find: The trans-atlantic data privacy dispute territorial jurisdiction and global governance. *Review of International Studies.*

Kubli-García, Fausto. 2009. *Régimen jurídico de la bioseguridad de los organismos genéticamente modificados*. México. Instituto de Investigaciones Jurídicas - UNAM.

LaSalle, Ferdinand. 1862. ¿Qué es una Constitución?

Lindblom, Charles E. 1959. *The Science on "Muddling Through".* Public Administration Review. Vol. 19, No. 2. USA. Blackwell Publishing on behalf of the American Society for Public Administration

Linder S. y Peters B. 1987 *A design perspective on policy implementation: the fallacies of misplaced prescription.* Review of Policy Research. Policy Studies Organization. Pág. 459 – 475.

Lowi, T. 1972. *Four Systems of Policy, Politics and Choic*. En *Public Administration Review*, número 32, pp. 298-310. USA.

Luna Pla, Issa. 2013 [2009]. *Movimiento social del derecho de acceso a la información en México*. Instituto de Investigaciones Jurídicas, UNAM. 1ª reimpresión.

Magaloni Kerpel, Ana Laura. 2009. ¿Por qué la Suprema Corte no ha sido un instrumento para la defensa de Derechos Fundamentales? México. Instituto de Investigaciones - Jurídicas UNAM.

Magaloni Kerpel, Ana Laura. 2011. La Suprema Corte y el obsoleto sistema jurisprudencial constitucional. Cuadernos de Trabajo número 57. Mèxico. Centro de Investigación y Docencia Económicas.

Majone, Giandomenico (ed.). 1990. *Deregulation or Re-regulation?: Regulatory Reform in Europe and the United States*. London. New York St Martin's Press.

Mantilla, Trolle. 2008. Los censos (población, económicos y agropecuarios). Curso intensivo de Formación de Estadísticas de Genero. Mèxico. INEGI.

Margetts, Helen y Patrick Dunleavy. 2013. *The second wave of digital-era governance: a quasi-paradigm for government on the Web.* Philosophical Transactions: Mathematical, Physical and Engineering Sciences. Vol. 371, número 1987. USA. Web science: a new frontier (28 March 2013), pp. 1-17.

Martínez, Macarena. 2016. Jurisprudencia social del tribunal europeo de derechos humanos. Revista Jurídica de los Derechos Sociales. Vol. 6 No. 1 Pag.355 -387. Disponible en: file:///C:/Users/ssalg/Downloads/1715-Texto%20del%20art%C3%ADculo-5411-2-10-20160603.pdf

Mauricio Merino. 2013. *Políticas Públicas. Ensayo sobre la intervención del Estado en la solución de problema públicos.* México. Centro de Investigación y Docencia Económicas. 192 pp.

Mayer-Schönberger, Viktor. 1997. *Generational Development of Data Protecton in Europe.* In

Agre–Rotenberg. pp. 219-241. Agre, Philip E. y Totenberg, Marc. Technology and privacy: the new landscape. USA. MIT Press Cambridge.

Merino, Mauricio, Guillermo M. Cejudo, David Arellano, Teresa Bracho, María A. Casar, José R. Gil-García, Claudia Maldonado, Judith Mariscal, Lucrecia Santibáñez y Laura Sour. 2010. *Problemas, decisiones y soluciones*. Enfoques de política pública. México. Fondo de Cultura Económica y Centro de Investigación y Docencia Económicas.

Mill, John Stuart. 1997. *Sobre la libertad.* Madrid. Alianza.

Murphy D. Sean. 2001. U.S.-EU "Safe Harbor" Data Privacy Arrangement. *The american journal of international law.* Volume 95. 1. Pág. 156 – 159. USA. American Society of International law.

Narro, Robles José y David Moctezuma Navarro. 2012. *Analfabetismo en México. Una deuda social.* Mèxico. INEGI. Disponible en línea. http://www.inegi.org.mx/eventos/2013/RDE_07/Doctos/RDE_07_Art1.pdf

North, Douglass C. 1990. *Institutions, Institutional Change and Economic Performance.* USA. Cambridge University Press.

O'Donnell, Guillermo. 2008. *Democracia y Estado de Derecho.* En Ackerman, John. Más allá del acceso a la información. México. Siglo XXI Editores. Pág. 89-99.

Olea Rodríguez, H. 2007. *Derechos Humanos y Migraciones. Un nuevo lente para un viejo fenómeno.* Anuario de Derechos Humanos. Chile. Centro de Derechos Humanos.

Ornelas Núñez, Lina y Sergio López Ayllón. 2007. *La recepción del derecho a la protección de datos en México: breve descripción de su origen y estatus legislativo, Memorias del II Congreso Mexicano de Derecho Procesal Constitucional*. Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México. Procesal Constitucional. México. En Cámara de Diputados e Instituto Federal de Acceso a la Información pública y Protección de Datos (IFAI). 2010. Protección de datos personales. Compendio de lectura y legislación. México, Tiro Corto editores.

Ornelas y Piñar. 2013. *La protección de datos personales en Mèxico.* México. Tirant lo Blanch.

Ornelas, Lina, Miguel Recio y Víctor Chapela. 2013. En Canal Once. Video Espiral, Privacidad y protección de datos personales. 17 de abril de 2013. Disponible en: https://www.youtube.com/watch?v=5b6l2dkf5Hs

Parra, Noriega L. Gustavo. 2008. *Avances y retos en materia de protección de datos personales en la legislación mexicana.* México. Instituto Estatal De Acceso A La Información Pública

- Oaxaca. Disponible en http://Www.Ieaip.Org.Mx/Biblioteca_Virtual/Nuevo/Datos/20personales/Avances/y/retos/en/ma teria/de/proteccion/de/datos/personales/en/la/legislacion/mexicana.Pdf

Perrow, Charles. 1984. *Normal Accidents: Living With High Risk Technologies.* (Revised edition, 1999). USA. Princeton University Press.

Piñar Mañas, José Luis. 2008. *¿Existe privacidad?* Lección magistral impartida en la Apertura Solemne del Curso Académico en la Universidad San Pablo-CEU de Madrid. España. En Cámara de Diputados e Instituto Federal de Acceso a la Información Pública y Protección de Datos Personales (IFAI). 2010. *Protección de datos personales. Compendio de lectura y legislación.* México, Tiro Corto Editores.

Pressman, Jeffrey L. y Aaron Wildavsky. 1979. *Implementación.* México. FCE.

Privacy Act Canadá. 2011. *The personal Information Protection and Electronic documents Act. (PIPEDA). Office of the privacy commissioner of Canada*.

Recio Gayo, M. 2013. *La transferencia nacional e internacional de datos personales, en La Protección de Datos Personales en México*. México. Tirant lo Blanch.

Revenga Sánchez M. 2001. Servicios de inteligencia y derecho a la intimidad", en REDC, núm. 61.

Rodotà, Stefano. 2003. *Democracia y protección de datos.* Cuadernos de derecho público, número. 19-20, Madrid, pp. 15-26. Consultado en mayo de 2015 en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/DemocraciaMadrid__mayo_05.pdf y http://www.ictparliament.org/sites/default/files/1pf_RodotaCaseStudies.pdf

Rodotá, Stefano. 2004. *Tecnología y Derechos Fundamentales.* Datospersonales.org. Revista de la Agencia Española de Protección de Datos de la Comunidad de Madrid, número 8, Madrid.

Rodotá, Stefano. 2012. *Hay que oponerse a ser perfilado por razones de mercado o por poderes políticos*. Consultado el 21 de agosto del 2012 en: http://www.yorokobu.es/stefanorodota/

Román Sánchez, Carlos Vital. 2014. *Derecho a la privacidad, a la protección de datos y a la información en México.* México. Thomson Rauters.

Rubenfel, Jed. 1989. *The Right to Privacy*. Harvard Law Review. USA. The Harvard Law Review Association. Pàg. 737-807.

Schmidth-Eenboom, Erick. 2001. “The Bundesnachrichtendienst, the Bundeswehr and Sigint in the Cold War and After”, en Aid M. Matthew, Wiebe Cees, Christopher Andrew, 2001, Secrets of Signals Intelligence During the Cold War and Beyond. Routledge. Reprint 2004 edition, pág. 129– 177.

Schneider e Igram. 1993. *Social Construction of Target Populations: Implications for Politics and Policy.* The American Political Science Review. Vol. 87, No. 2. Pág. 334 – 347. USA. American Political Science Association.

Secretaría de Economía. 2013. Estudio de autorregulación en materia de privacidad y protección de datos personales en el ámbito de las TI. 5ª versión. PROSOFT 2.0, CANIETI y SE.

Servicio de Administración Tributaria. 2016. Solicitud de la firma electrónica avanzada. Términos y condiciones. México. Disponible en: www.sat.gob.mx

Servicio de Administración Tributaria. 2019. *Datos abiertos*. México. Disponible en: http://omawww.sat.gob.mx/cifras_sat/Paginas/datos/vinculo.html?page=giipTipCon.html

Singer, Peter. 1995. *Repensando la vida y la muerte: El colapso de nuestra ética tradicional.* USA. Oxford.

Tamayo y Salmorán, Rolando. 2003. *Razonamiento y argumentación jurídica: el paradigma de la racionalidad y la ciencia del Derecho.* México. UNAM – Instituto de Investigaciones Jurídicas

US. Department of Commerce. 2016. *Privacy Shield Framework.* [online] Disponible en: https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg

Uvalle, Ricardo. 2011.*Las políticas públicas en el arquetipo de la gobernanza democrática*. En Revista *del CLAD Reforma y Democracia.* No. 50 Caracas, Venezuela. Pág. 1 – 13.

Uvalle, Ricardo. 2017. “El control del poder en México: Una perspectiva desde la rendición de cuentas”, en Ricardo Uvalle Berrones y Maximiliano García Guzmán (coords.). *Sentido y alcance de la rendición de cuentas.* México. Universidad Nacional Autónoma de México, Facultad de Ciencias Políticas y Sociales, Editorial Tirant Lo Blanch. Pág. 221 -252.

Velasco, San Martín, Cristos. 2003. *Privacidad y protección de datos personales en Internet. ¿Es necesario contar con una regulación específica en México?* [online], México. Boletín de Política Informática, número 1, Disponible en: http://www.inegi.gob.mx/inegi/contenidos/espanol/prensa/contenidos/Articulos/tecnologia/libertad.pdf

Viggiola E, Lidia y Eduardo Molina Quiroga. 1999. *Tutela de la autodeterminación informativa.*

Aproximación a una regulación eficaz del tratamiento de datos personales. Ponencia presentada al Congreso Internacional "Derechos y Garantías en el Siglo XXI" de la Asociación de Abogados de Buenos Aires. Documento electrónico consultado en: http://www.aaba.org.ar/bi151302.htm

Wacks, Raymond. 2010. *Privacy: A Very Short Introduction*. USA. Oxford University Press.

Warren, Samuel y Louis Brandeis. 1995. *El derecho a la intimidad*. Madrid, España. Cívitas. Traducción de Benigno Pendás y Pilar Baselga

Weeramantry, Christopher Gregory. 1990. *Human Rights and Scientific and Technological Development.* USA. The United Nations University

Weeramantry, Christopher Gregory. 1993. Impact of Technology on Human Rights: Global Case Studies, United Nations University Press, 1993, work edited for and commissioned by the United Nations Human Rights Commission and the United Nations University.

Weimer D. y Vining A. 2011. *Policy Analysis: Concepts and Practice.* Universidad de Michigan.USA. Longman.

Weinstein, Jason. 2013. *Doesn't Have a National Data Protection Authority? Privacy Perspectives.* Oct 16, 2013. The U.S. Disponible en línea: https://privacyassociation.org; https://www.ftc.gov/es/enforcement/statutes/federal-trade-commission-act

Wildavsky, Aaron. 1979. *The Art and Craft of Policy Analysis.* UK. Palgrave Macmillan UK.

Yee, George (ed.). 2006. Privacy Protection for E-services. Hershey, Pa. Idea Group Publishing.

Yves Mény y J.C. Thoening. (1992) *Las políticas públicas*. España, Ariel.

CONVENIOS Y TRATADOS

Agencia de Protección de Datos de España (AGPD). 2009. Resolución en Madrid. Estándares Internacionales sobre protección de datos personales y privacidad. Disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf

Asamblea General de las Naciones Unidas (AGNU). (1948) Declaración Universal de los Derechos Humanos. Consultado el 14 de diciembre de 2010. Disponible en http://157.150.195.10/es/documents/udhr/

Consejo de Europa. (1981) "Convenio 108, para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal". En Cámara de Diputados, e

Instituto Federal de Acceso a la Información pública y Protección de Datos Personales. (2010) Protección de datos personales. Compendio de lecturas y legislación. México, Tiro Corto editores. Pp. 249- 262.

European Commission. (2010) Legislation. [online], European Comisión Justice, disponible en: http://Ec.Europa.Eu/Justice/Policies/Privacy/Instruments/Index_

Foro De Cooperación Económica Asia Pacífico. (1998). "Marco de Privacidad". En Cámara de Diputados e Instituto Federal de Acceso a la Información pública y Protección de Datos Personales (IFAI). 2010. Protección de datos personales. Compendio de lectura y legislación. México, Tiro Corto editores pp. 307-317.

Organización para la Cooperación y el Desarrollo Económico. 1980. Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales. Disponible en http://www.csae.map.es/csi/pdf/OCDE_directrices_privacidad.pdf, consultado en diciembre de 2010.

Organización de las Naciones Unidas (1990) "Directrices para la regulación de los archivos de datos personales informatizados". Disponible en: Cámara de Diputados e Instituto Federal de Acceso a la Información pública y Protección de Datos (IFAI). 2010. Protección de datos personales. Compendio de lecturas y legislación. México, Tiro Corto editores. Pp. 267-70.

Parlamento Europeo (2016) Reglamento del Parlamento Europeo y del Consejo UE 2016/679

Parlamento Europeo. (1995) Directiva 95/46/CE, "Protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos". Disponible en: Cámara de Diputados e Instituto Federal de Acceso a la Información pública y Protección de Datos Personales. (2010) Protección de datos personales. Compendio de lectura y legislación. México, Tiro Corto editores. Pp. 271-305.

Red Iberoamericana de Protección de Datos. (2007). "Directrices para la armonización de la protección de datos en la comunidad iberoamericana". En: IFAI, Cámara de Diputados. 2010. Protección de Datos. Compendio de lecturas y legislación. México, Distrito Federal.

ENTREVISTAS

1. Alfredo Reyes Krafft, Especialista del sector privado (BBVA), 4 de diciembre de 2014.
2. Edgardo Martínez, Director de Regulación, IFAI, 7 de noviembre de 2014.

3. Fernando Martínez Coss, funcionario del Servicio de Administración Tributaria, 19 de agosto de 2016.
4. Gustavo Parra Noriega, Coordinador de Protección de Datos, IFAI, 24 de noviembre de 2014.
5. Issa Luna Pla, Académica del Instituto de Investigaciones Jurídicas de la UNAM, 18 de noviembre de 2014.
6. Jacobo Esquenazi, Oficina de Privacidad de HP para las Américas, 15 de diciembre de 2014.
7. José Luis Piñar Mañas, Consultor y académico internacional, 2 de octubre de 2014.
8. María Marván Laborde, Excomisionada del IFAI, académica del Instituto de Investigaciones Jurídicas de la UNAM, 29 de octubre de 2014.
9. Miguel Recio Gayo, Consultor y académico internacional, 19 de noviembre de 2014.