

FACULTAD LIBRE DE DERECHO DE MONTERREY

LICENCIATURA EN DERECHO



**SI NO PAGAS POR EL SERVICIO EL PRODUCTO ERES TÚ: ANÁLISIS DE LA
LEGALIDAD DE LA COMPRA, VENTA Y TRATAMIENTO DE LOS DATOS
PERSONALES EN LA ERA DE LOS “DATA BROKERS”.**

**TESIS QUE EN OPCIÓN A TÍTULO DE
LICENCIADO/A EN DERECHO**

PRESENTA: ANA KAREN MONCAYO LIVAS

**ASESOR DE FONDO: MTRO. ALEJANDRO SÁNCHEZ MÚJICA
ASESOR DE FORMA: MTRO. JOSÉ FABIÁN RUIZ**

SANTA CATARINA, N.L.

OCTUBRE, 2024

Santa Catarina, Nuevo León, a 3 de octubre de 2024



AGRADECIMIENTOS

Al inicio de cada semestre, los maestros nos planteaban a los estudiantes una serie de preguntas para conocernos, o acordarse de nuestros nombres. Entre ellas una muy común fue, ¿tienes familiares abogados? Yo no tengo familiares abogados, pero a lo largo de mi carrera he tenido el enorme privilegio de estar rodeada de los mejores que pudiera haber conocido. Tanto dentro de las aulas como por consecuencia de pertenecer a las mismas, me he topado con abogados que han sido una parte íntegra de mi formación no solo profesionalmente, sino a nivel personal. Quisiera agradecer a todos mis maestros de la Facultad, porque en retrospectiva puedo ver que a cada uno le aprendí una lección ajena a el material de sus clases. Tengo la certeza de que la dedicación, vocación, y empatía que existe dentro del cuerpo docente de la Facultad Libre de Derecho de Monterrey es una que no puede ser replicada en ningún otro lado.

Ahora bien, a pesar de que no tengo familiares abogados, considero que sí tengo seres queridos que ejemplifican características del tipo de abogada que quisiera ser. Es por esto que quisiera tomarme el tiempo de agradecerles por darme los estándares a los cuáles quisiera aspirar. A mi mamá, por siempre hacer las cosas con amor y compasión. A mi papá, por ser firme en sus convicciones. A mi abuela, por ser fuerte y perseverante. A mi abuelo, por ser alguien que siempre está dispuesto a escuchar a los demás. A mis hermanas por ser fieles a las cosas que les importan. Y por último a mis amigas, por ser apasionadas por lo que hacen.

Infinitas gracias tanto a la Facultad como a mis seres queridos por ser la familia abogada que nunca pensé que tendría.

RESUMEN

En este trabajo, se analiza la legalidad de la compra, venta, y tratamiento de los datos personales a través de los “data brokers”. Desde una perspectiva jurídica, se analizan los derechos de los cuales son titulares los usuarios del internet con respecto de sus datos personales. También, se analizarán los estándares regulatorios que han sido observados a nivel internacional. Para lograr lo anterior, se examinará el derecho internacional, así como distintas sentencias para comprender los lineamientos que deberán de respetar las plataformas digitales con respecto de la protección de datos personales. También, se discuten casos trascendentales con respecto del derecho a la vida privada para lograr comprender los riesgos y retos que enfrentan los usuarios al acceder a compartir sus datos. Al final de este trabajo, se concluye que deberán de suceder cambios significativos dentro de la legislación en materia de protección de datos para asegurar que los mismos sean vistos como derechos fundamentales que no podrán ser cedidos en el nombre de los “términos y condiciones”.

Palabras clave: privacidad de datos- “data brokers” – derecho a la vida privada- perfilamiento- términos y condiciones

ABSTRACT

This paper strives towards analyzing the legality of the practices conducted by data brokers when it comes to buying, selling, and giving treatment to personal data. From a legal standpoint, we will analyze the rights that internet users hold in regard to their personal information, as well as the regulatory standards that are set on an international level. To do so, we will be examining international law, as well as established court rulings to understand the guidelines that digital platforms must observe when it comes to protecting data. We will also discuss transcendent cases regarding privacy law to better understand the risks and challenges users face when accepting to share their data. At the end of this paper, we conclude that significant changes must be made on a legislative level to ensure that users privacy is

seen as a fundamental right that can not be handed over to digital platforms in the name of “terms and conditions”.

Keywords: data privacy- “data brokers” – right to privacy- profiling- terms and conditions

ÍNDICE

INTRODUCCIÓN.....	1
MARCO CONCEPTUAL	5
CAPÍTULO I.....	9
MARCO TEÓRICO	9
1. 1. PANORAMA DE LA VENTA DE DATOS PERSONALES.	9
2. 2. CONCEPTO DE DATOS PERSONALES	15
CAPÍTULO II.....	29
CASOS TRASCENDENTES	29
3. 1. GOOGLE VS. ESTADO DE CALIFORNIA.	29
4. 2. FTC VS. FLO HEALTH, INC.	35
CAPÍTULO III	42
ANÁLISIS DE LAS PROTECCIONES ACTUALES Y SUS INEFICIENCIAS.....	42
1. DE LA DISTINCIÓN DE LOS DATOS SENSIBLES.....	42
2. DE LOS DERECHOS ARCO	45
3. DEL INAI.....	48
CAPÍTULO IV	55
¿QUÉ TIENE QUE CAMBIAR?	55
1. CAMBIAR LA POSIBILIDAD DEL “OPT- OUT”	57
2. AMPLIACIÓN DE FACULTADES DEL INAI.....	59
3. REFORMA AL ARTÍCULO 9 DE LA LFPDPPP Y SU RESPECTIVO MANUAL DE OPERACIONES.	60
CONCLUSIONES.....	64
BIBLIOGRAFÍA	69

INTRODUCCIÓN

Es ordinario mencionar algún producto y posteriormente verlo anunciado a través de nuestras redes sociales. Asimismo, regularmente accedemos a compartir nuestras fotos, o nuestra ubicación a tiempo real con aplicaciones que quizás y nunca hemos ni siquiera abierto. En nuestras cuentas de Netflix, se podrá observar que las películas en el menú de opciones tienen junto a su título un porcentaje que indica su compatibilidad con nuestro gusto personal. Spotify nos genera playlists con base en los artistas que escuchamos y nuestros hábitos musicales. Inclusive existen aplicaciones como Hinge dedicadas a encontrar nuestra pareja ideal con la que podremos tener hobbies, preferencias, e inclusive ideologías en común. Esto no es una coincidencia, sino, el producto de una práctica que comenzó desde antes de los inicios del internet: la venta de datos personales.

El fenómeno de la venta de nuestros datos personales es uno que, a lo largo de esta era tecnológica, ha sido tácitamente aceptado, poco cuestionado, y aún así, en la mente de muchos. En un estudio realizado por Norton AntiVirus, se reveló que el 80% de los consumidores temen por la privacidad de sus datos personales, y que el 70% reiteran estar más preocupados que nunca.¹

Sin embargo, a pesar del escepticismo del público general con respecto del manejo de sus datos personales, sabemos que hay un aproximado de 5.35 miles de millones de usuarios del internet y redes sociales a nivel global, es decir, más del 60% del mundo.² Dicho lo anterior, si cerca a la mitad de la población se encuentra consternada por las prácticas de almacenamiento y manejo de datos personales, es indispensable dar a conocer los alcances de las mismas, así como cuestionar su legalidad.

¹ Harris Insights & Analytics, LLC “**2022 Cyber Safety Insights Report- Global Results**”. Estados Unido: Enero 2022. Disponible en línea: Norton Life Lock <<https://www.nortonlifelock.com/us/en/newsroom/press-kits/2022-norton-cyber-safety-insights-report-special-release-online-creeping/>> (Consulta: Febrero 2024)

² Petrosyan, Ani “**Worldwide digital population 2024**”. Estados Unidos: Octubre 10, 2024. Disponible en línea: Statista <<https://www.statista.com/statistics/617136/digitalpopulationworldwide/#:~:text=Worldwide%20digital%20population%202024&text=As%20of%20January%202024%2C%20there,population%2C%20were%20social%20media%20users>> (Consulta: Octubre 2024)

La venta de datos personales, como sugiere el nombre, es una práctica transaccional. A través de esta, las empresas logran comprender de una mejor manera los deseos y las necesidades de sus usuarios quienes, en turno, tendrán acceso a interfaces más eficientes y personalizadas. En términos generales, podemos decir que la venta de datos juega un papel importantísimo en los mercados actuales. Pero como todo, puede ser una herramienta que funge como espada de doble filo si no es regulada correctamente y tomando en cuenta los derechos fundamentales de sus usuarios. Así como la venta de datos personales puede presentar un beneficio comercial, también puede implicar injerencias graves en las esferas jurídicas del usuario. Estas injerencias pueden variar desde un alza en tarifas de seguros médicos³, hasta al robo de identidad. Hace relativamente poco, Tesla anunció que estarían utilizando los datos de manejo de sus vehículos para fijar la tarifa del seguro de autos, por ejemplo.⁴

Si bien sabemos que existen términos y condiciones donde el usuario accede a compartir ciertos datos, ¿sabemos en realidad qué tipo de información estamos compartiendo? Todos estamos conscientes de la venta de datos. No es una novedad. Sin embargo existe esta idea de que cualquier inconformidad que se pueda tener en contra de la venta de datos puede ser superada por un singular argumento: nosotros ACEPTAMOS mediante distintos términos y condiciones a compartir estos datos. Inclusive ese argumento se ve acompañado por un argumento accesorio: quizás y si el usuario no fuera tan ignorante, pudiera haber leído los términos y condiciones, para en turno objetarlos. No hay fallas en esa lógica, pero como iremos viendo a lo largo de la investigación, hay ciertas cosas que simplemente no pueden ser toleradas bajo el supuesto de que nosotros lo aceptamos.

El fin de esta investigación es probar, que la venta de datos (por más beneficiosa y trivial que pueda parecer) muchas veces resulta en el tratamiento de datos sensibles- mismos

³ Allen, Marshall. “**Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates**”. Estados Unidos: Julio 17, 2018. Disponible en línea: **Pro Publica** < <https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates>> (Consulta: Febrero 2024)

⁴ Hill, Kashmir. “**Automakers Are Sharing Consumers’ Driving Behavior With Insurance Companies**”. Estados Unidos, Marzo 11, 2024. Disponible en línea: New York Times < <https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html>>

que constituyen datos médicos que por su naturaleza irrenunciable, no deben ser cedidos bajo la modalidad en la que lo hacemos actualmente.

Se estarán preguntando- ¿cómo pasamos de hablar de algoritmos de Spotify a datos médicos? ¿Qué tiene que ver una cosa con la otra? Se ha ido descubriendo que gracias a prácticas como el perfilamiento (y otras que vamos a explorar a continuación), todos los datos personales (hasta los más aparentemente banales) pueden ser convertidos en datos sensibles. En un ejemplo sumamente simplístico- consideremos un día típico como usuario de Google. Google podrá utilizar su rastreo de ubicación a tiempo real para determinar que un usuario acudió a la farmacia. Podrá utilizar su historial de búsquedas para saber que dicho usuario buscó sus síntomas en el navegador. Podrá igualmente captar la información que se encuentra en el recibo que fue mandado a su correo electrónico para determinar el medicamento que fue adquirido. Todos estos datos que fueron captados (muchas veces sin el conocimiento del mismo usuario) podrán en turno ser colocados en una base de datos que sirve para perfilar de la manera más específica a uno y cada uno de los usuarios del internet. Con la información proporcionada en esa simple visita a la farmacia, aunado a los datos existentes del usuario, quizás esa persona podría ser perfilada como una persona con indicios de diabetes o hipertensión. Este análisis podrá ser vendido (e históricamente, lo ha sido) a la aseguradora del usuario, quienes en turno podrán subir su tarifa de seguro de gastos médicos, tomando en cuenta su perfil de riesgo de salud. Todo esto para decir, que nuestros datos “triviales”, pueden llegar a ser tratados hasta convertirse en sensibles.

Tanto la legislación federal mexicana, como lo mencionado por distintos tratados internacionales indican que estos datos, por su naturaleza sensible, no deberán de ser tratados salvo en supuestos muy específicos que veremos adelante. Pero como iremos viendo, los datos no solamente son tratados, sino también son vendidos, sin nuestro consentimiento y en nuestro perjuicio.

Tomando en cuenta lo anterior, el presente trabajo busca realizar una investigación con respecto de la legalidad de la venta de datos personales a luz de las violaciones que se

incurren por compartir datos de índole médico. Para abordar este tema, se buscará determinar la naturaleza jurídica que comprende nuestra información sensible, para así, comprender los derechos que se deben de salvaguardar al compartirla con empresas.

Para efectuar este análisis, se comenzará dando a conocer las distintas figuras clave en el mundo de la venta de datos personales. Aquí, se entrará en contexto en cuanto a el negocio de los “Data Brokers”, y se dará a comprender cuáles datos estamos compartiendo, y con quién. Posteriormente, se realizará un estudio de la naturaleza jurídica tanto de los datos personales, como de los Avisos de Privacidad donde aceptamos (a veces sin saber) compartirlos. Comprendiendo la naturaleza jurídica de estas figuras, podremos realizar un derecho comparado utilizando normativa internacional para comprender los principios rectores de los datos personales a través del mundo.

MARCO CONCEPTUAL

El marco conceptual tiene por objeto exponer los términos definidos que serán utilizados frecuentemente a lo largo de la investigación. Los temas que serán enunciados serán aquellos que son un poco más específicos al tema de los datos personales, para no definir conceptos que deberían de ser conocidos por todo quien sabe de derecho. Algunos ejemplos de términos que quisiera definir incluyen; “Data Broker”, “Datos Personales”, “Big Data”, “De-identificación de Datos”, “Cookies” “Tracking” y demás. De igual manera, definir algunas entidades que tienen como objeto la protección de datos personales como el “INAI” para México o el “OAIC” para Australia.

A. Big data and analytics

En el presente trabajo, el término “big data” se comprenderá por los datos (ya sean de índole personal o no) de alto volumen, velocidad y variedad. Para efectos de esta tesis, se comprenderá que los datos recolectados por las empresas tecnológicas, (especialmente cuando se habla de la segmentación de clientes a mayoreo) se entenderán como “big data”.⁵

De igual manera, la palabra “analytics” en relación con el “big data” refiere a la examinación que se lleva a cabo para llegar a conclusiones en virtud de los datos que son procesados. El big data analytics se entenderá como el medio para llegar al fin que, en este caso, será la venta de datos (los datos se deberán de comprender antes de vender).⁶

B. Data brokers

Se podrán observar distintas definiciones para los “data brokers” a través de distintas jurisdicciones, sin embargo, la premisa es la misma. En el libro “Data Brokers in an Open Society” elaborado por la asociación Open Society Foundations, se define a la figura como

⁵ Fadler, Martin y Legner, Christine. “Data ownership revisited: clarifying data accountabilities in times of big data and analytics”. Reino Unido: 2022. Disponible en línea: Journal of Business Analytics, Taylor & Francis <<https://www.tandfonline.com/doi/full/10.1080/2573234X.2021.1945961#abstract>> (Consulta: Enero, 2024)

⁶ Loc. Cit.

“A company or business unit that earns it’s primary revenue by supplying data or inferences about people gathered mainly from sources other than the data subjects themselves.”⁷ En español, esto se traduce a “Una empresa o unidad de negocios que genera sus utilidades principalmente a través de proporcionar datos o inferencias acerca de personas, recolectados primordialmente por fuentes distintas a los mismos sujetos de los datos.”⁸

C. Pseudonymisation

Dentro de la legislación en materia de protección de datos personales se habla de la “de-identificación” de datos, este término se conoce también como “pseudonymisation” en el Reglamento General de Protección de Datos (ahora en adelante, GDPR) como lo siguiente: “The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person”.⁹ En español, esto se traduce a “El procesamiento de datos personales de tal manera en que los mismos no podrán ser atribuidos a un sujeto de datos específico sin el uso de información adicional, siempre y cuando dicha información se almacene separadamente y sea sujeto de medidas técnicas y organizacionales para asegurar que los mismos no sean atribuidos a una persona física identificada o identificable”.¹⁰ Como se menciona en la cita anterior, la “Pseudonymisation” es una práctica que se lleva a cabo para poder utilizar la información de los usuarios sin revelar su identidad.

D. Cookies

Las “cookies” son pequeños archivos que se comparten en nuestros dispositivos cuando accedemos a ciertas páginas de internet o aplicaciones. [Las cookies pueden ser propias o de terceras partes cuando son implementadas en páginas de internet ajenas con

⁷ Von Hoboken, Joris y Rieke, Aaron y Yu, Harlan y Robinson, David. **Data Brokers in an Open Society**. Open Society Foundation, London, 2016.

⁸ Esta traducción fue redactada por la autora de esta tesis.

⁹ **Reglamento General de Protección de Datos**. Unión Europea. (Vigente Mayo 25, 2018 / Mayo 9 2023)

¹⁰ Esta traducción fue redactada por la autora de esta tesis.

finalidad de anunciar algún producto o servicio (anuncios pop up, por ejemplo)] Las cookies son utilizadas para que las páginas web tengan memoria acerca de la navegación de la misma por parte del usuario.¹¹

E. Profiling

De igual manera, el GDPR define al “profiling” como lo siguiente;

“‘Profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.”¹²

Con esta definición, podemos comprender que el “profiling” sirve para relacionar algún dato determinado con algún tipo de usuario. Como se irá mencionando a lo largo de esta investigación, la venta de datos es utilizada principalmente con fines publicitarios. Es por esto, que la práctica de “profiling” juega un rol importante dentro de la venta de datos, ya que permite a los compradores de datos a poder optimizar sus estrategias de marketing y ventas.

F. Contrato de Adhesión

Con respecto de los contratos de adhesión, la Ley Federal de Protección al Consumidor proporciona una definición comprensiva en su artículo 85 donde se establece lo siguiente:

*“ARTÍCULO 85.- Para los efectos de esta ley, se entiende por contrato de adhesión el **documento elaborado unilateralmente por el proveedor, para establecer en formatos uniformes los términos y condiciones aplicables a la adquisición de un producto o la prestación de un servicio**, aun cuando dicho documento no contenga todas las cláusulas ordinarias de un contrato. Todo contrato de adhesión celebrado en territorio nacional, para su validez, deberá estar escrito en idioma español y sus caracteres tendrán que ser legibles a simple vista y en un tamaño y tipo de letra uniforme. Además, no podrá implicar*

¹¹ Davara, Isabel. “Diccionario de Protección de Datos Personales: Conceptos Fundamentales. México: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Primera ed. Noviembre del 2019.

¹² Reglamento General de Protección de Datos. Unión Europea. (Vigente Mayo 25, 2018 / Mayo 9 2023)

prestaciones desproporcionadas a cargo de los consumidores, obligaciones inequitativas o abusivas, o cualquier otra cláusula o texto que viole las disposiciones de esta ley.”

CAPÍTULO I

MARCO TEÓRICO

Este capítulo sienta las bases teóricas necesarias para comprender a detalle el fenómeno de la venta de datos personales. En los siguientes apartados, se buscará dar a entender la razón por la cual la compra y venta de datos es de los negocios más rentables en la actualidad. Este capítulo servirá para comprender los efectos (tanto positivos como adversos) que ha tenido la venta de datos personales sobre los mercados, y los consumidores. Para lograr lo anterior, se entrará en materia para comprender a profundidad cuáles son los datos que se están utilizando y para qué se utilizan (qué se logra mediante venta de datos). Finalmente, se expondrán también las prácticas que son utilizadas para optimizar la venta de datos, para dar a entender que esta práctica, por más antigua que sea, afecta a los consumidores de maneras que pasan totalmente desapercibidas.

1. PANORAMA DE LA VENTA DE DATOS PERSONALES.

La venta de datos personales (o el data brokerage) es un tipo de transacción que (en términos generales), se lleva a cabo con la finalidad de conocer al consumidor, y en turno comprender sus necesidades. Al conocer al consumidor, las empresas podrán crear productos o servicios que atienden a sus necesidades, a la vez mejorando ventas y generando mayor utilidad. En la actualidad, conocer al consumidor se podrá ver expresado a través de los anuncios personalizados que aparecen constantemente. En la era de “influencers”, se vuelve claro que los anuncios y la publicidad juegan un rol importantísimo en el comercio. Tan es así, que empresas multinacionales como Google reportan que el 80% de sus ingresos son obtenidos en virtud de los anuncios que demuestran en sus páginas, sobrepasando un total de \$237 mil millones de dólares al cierre del 2023.¹³

¹³ Bianci, Thiago “Advertising revenue of Google from 2001 to 2023”. Brazil: Mayo 22, 2024. Disponible en línea: Statista <<https://www.statista.com/statistics/266249/advertising-revenue-of-google/>>Consulta: Abril 2024)

A la luz de esto, vender datos personales se ha vuelto no solamente popular, sino indispensable para la supervivencia de miles de empresas, tanto las que fungen como plataformas para los anuncios como las que se anuncian en plataformas ajenas. De igual manera, hemos llegado al punto donde la única manera para asegurar que un anuncio llegue a los ojos u oídos correctos, es a través de la colección de información de los usuarios.

A continuación, se entrará en detalle en cuanto al “Data Brokerage” y la Venta de Datos personales para posteriormente dar a comprender de donde viene y como se utiliza hoy en día.

1.1 ANTECEDENTES.

En términos simplificados, la venta de datos personales conlleva la transacción que se lleva a cabo cuando se venden datos que han sido recolectados. Esta información puede ser segmentada o categorizada de la manera que sea de mayor conveniencia para el comprador, quien, en turno, podrá utilizar los hallazgos como quiera (aunque generalmente se utiliza con fines de mejorar ventas o publicidad). Esta definición que se ha elaborado, no menciona el lado digital de esta transacción. Esto es porque la venta de datos tiene inicios en épocas anteriores a la era tecnológica. De hecho, se considera que esta es una práctica que comenzó en los años 70, es decir, alrededor de una década antes del nacimiento del internet.

La venta de datos como la conocemos, fue producto de una práctica introducida por la empresa Claritas. Esta empresa desarrolló un producto denominado PRIZM¹⁴, mismo que sigue siendo utilizado hoy en día. PRIZM era un programa de segmentación cuya finalidad era categorizar a los clientes de determinadas empresas para poder optimizar ventas. Este programa, desarrollado en el año 1974 por el sociólogo Jonathan Robin, fue el pionero en encontrar correlaciones entre la información disponible acerca de los clientes con sus gustos y preferencias. Puesto que en ese entonces era normal recibir catálogos y periódicos por

¹⁴ Office of Oversight and Investigations Majority Staff. **A Review of the Data Broker Industry: Collection, Use and Sale of Consumer Data for Marketing Purposes**. 18 de diciembre del 2013. p. 23. Disponible en línea: Committee on Commerce, Science, and Transportation. United States Senate. <<https://www.commerce.senate.gov/services/files/0d2b3642-6221-4888-a631-08f2f255b577> > (Consulta: Marzo 2024)

correo, Robin consideró que el código postal de una persona cobraba mucha más relevancia de lo que se suponía anteriormente. De igual manera, con la introducción de los códigos postales en el 1963, comenzaron los censos de población, que también fueron utilizados como indicadores para el programa.

Se consideraba que al conocer de cierta información básica acerca de los clientes, se podría predecir sus gustos y comportamientos. A diferencia de la venta de datos contemporánea, PRIZM dependía de información de acceso público. Los datos que eran recolectados no eran sensibles, sino, datos que pudieran ser conocidos por cualquiera que se diera la tarea de hacerlo (ya sea acudiendo a los archivos públicos o inclusive cualquier biblioteca). Utilizando factores como códigos postales, edad, nacionalidad, género, y nivel socioeconómico, PRIZM podía segmentar clientes y arrojar predicciones acerca de las preferencias de un determinado mercado.¹⁵

Es claro que la venta de datos ha cambiado drásticamente con el uso del internet, y más aún, con el auge de las redes sociales. Las predicciones arrojadas por programas como PRIZM no tendrían la exactitud de alguna predicción arrojada por un programa de segmentación actual. Esto se debe en parte, a lo accesible que se ha vuelto la información sensible del público general para quien la busca. Claramente, es una cosa predecir el comportamiento de un determinado grupo en función de un factor como edad, y otra muy distinta predecirlo con base en sus búsquedas en Pinterest.

1.2 CONTEXTO HISTÓRICO ACTUAL.

Como se ha ido exponiendo, la venta de datos es una práctica que ha ido evolucionando drásticamente desde sus inicios. Esto en función de la naturaleza de la

¹⁵ Office of Oversight and Investigations Majority Staff. **A Review of the Data Broker Industry: Collection, Use and Sale of Consumer Data for Marketing Purposes**. 18 de diciembre del 2013. p. 23. Disponible en línea: Committee on Commerce, Science, and Transportation. United States Senate. <<https://www.commerce.senate.gov/services/files/0d2b3642-6221-4888-a631-08f2f255b577> > (Consulta: Marzo 2024)

información que se puede conocer acerca de un cliente actualmente. En este apartado, se dará a entender el contexto actual de la figura a tratar a través de un desglose de los supuestos en los que se utiliza la venta de datos personales.

Las plataformas digitales han jugado un rol importante en la obtención de datos personales. Dejando a un lado los datos que los data brokers pueden obtener mediante métodos de rastreo, cookies, y términos y condiciones engañosos, es notorio que como usuarios hemos ido desarrollando huellas digitales extensas de manera inconsciente. Compartir cada movimiento con nuestra familia y amigos vía redes sociales es algo que se ha vuelto costumbre. Se han creado tantas plataformas nuevas con tantos nichos distintos que el problema ya no solamente gira en torno a las aplicaciones de Meta. Por lo menos partiendo de mi propia experiencia, puedo afirmar que mi teléfono sabe absolutamente todo de mí.

Aunado a las plataformas típicas donde compartimos nuestras imágenes, videos, e inclusive ubicación, hay otras aplicaciones que también deberán de ser tomadas en cuenta al hablar de la huella digital. Yo tengo una cuenta de Letterboxd, una aplicación con millones de usuarios donde las personas documentan las películas que están viendo en el momento, y comparten sus reseñas. Utilizo esa cuenta religiosamente, así que cualquier persona física o moral que tenga la intención de rastrear mis hábitos cinemáticos podrá saber exactamente en qué fecha vi qué película y qué pensé de ella. En aplicaciones como Pinterest mi huella digital es tan extensa que un extraño pudiera encontrar hasta el tipo de arreglo de flor que planeo tener en mi boda. En Spotify mis seguidores pueden ver las canciones que estoy escuchando en tiempo real, así como las playlists que sigo o elaboro. Si bien reconozco que esto es evidencia anecdótica, también reconozco que hay muchos usuarios que, como yo, disfrutan compartir lo que les gusta. Pero lo que estos usuarios quizás no contemplan, es la cantidad de información que se puede extraer acerca de una persona en función de sus publicaciones. A esto (como se mencionó en la introducción) se le llama “profiling”.

Si bien en el apartado anterior se partió de la base de que la venta de datos tiene como objeto la segmentación de clientes, también sabemos que se utiliza información para atribuir

ciertas características a ciertos grupos de personas. Así como los algoritmos en redes sociales pueden utilizar el contenido que consumes para arrojarle aún más contenido parecido, el profiling sirve para predecir comportamientos de las personas dependiendo del grupo en el que se encuentran. Por ejemplo, si una persona moral vigila mis hábitos tecnológicos y ve que soy fiel seguidora de Taylor Swift, pudiera esta considerar que soy parte de un grupo de personas que buscarán vuelos a su concierto más cercano. Esta agrupación de potenciales compradores podrá ser enlistado y vendido a una aerolínea. Posteriormente, utilizando esta información, esa misma aerolínea podrá comenzar a mandarme anuncios para incentivar a comprar un vuelo al concierto de Taylor Swift.

Lo último era solo un ejemplo, pero para aterrizar la práctica del profiling, utilizaremos el catálogo de productos publicado por la empresa data broker “Acxiom”. La empresa se describe como lo siguiente;

“We enable people-based marketing everywhere through a simple, open approach to connecting systems and data to drive better customer experiences for people and greater ROI for business. A leader in identity, customer data management and the ethical use of data for more than 50 years, Acxiom now helps thousands of clients and partners around the globe work together to create millions of better customer experiences, every day.”¹⁶

“(Nosotros habilitamos publicidad basada en personas por todos lados a través de un enfoque simple y abierto para conectar sistemas y datos para impulsar mejores experiencias para los usuarios y mejor rendimiento para los negocios. Un líder en el manejo de datos de identidad de usuarios y en el uso ético de datos por más de 50 años, Acxiom ahora ayuda a miles de clientes y socios de todo el mundo a trabajar juntos para crear millones de mejores experiencias de clientes todos los días).”¹⁷

Como se menciona, este tipo de empresas tienden a girar en torno a optimizar ventas de terceros bajo la premisa de que esto podrá ser logrado a través de una mejor experiencia para el usuario. En el caso de Acxiom, es una empresa reconocida globalmente por trabajar con marcas internacionales (L’oreal , Chase, Discover , Citigroup y Transunion, para nombrar un poco) para segmentar sus clientes y con base en ello, estructurar recomendaciones de marketing. Para dar a conocer los alcances de sus servicios, Acxiom

¹⁶ Acxiom. “Acxiom consumer data products catalog [PDF]”, p. 29-40. Disponible en línea: Acxiom <<https://ia801900.us.archive.org/14/items/187222488-acxiom-consumer-data-products-catalog/187222488-Acxiom-Consumer-Data-Products-Catalog.pdf>> Estados Unidos, 2023 (Consulta: Febrero 2024)

¹⁷ Esta traducción fue redactada por la autora de esta tesis.

publicó un catálogo titulado “Consumer Data Products Catalog: The Power of Insight”. A pesar de que el catálogo comprende las prácticas de una sola empresa de data broking, es muy ilustrativo del rol tan importante que juega el profiling dentro de la venta de datos.

El catálogo habla del uso del “infobase data enhancement” dentro de sus prácticas. Esta es la capacidad que tiene la empresa de obtener datos y categorizarlos de maneras muy específicas. El infobase data enhancement también permite a los clientes de Acxciom a encontrar la fuente de distintos tipos de datos (es decir, el origen de la información que es arrojada).

También, se muestran las categorías de datos que puede obtener Acxciom acerca de los clientes de las empresas a quienes le prestan servicios. Algunas categorías de datos incluyen: datos de comportamiento del cliente, datos de características individuales del cliente, datos de viajes del cliente, datos de uso de tecnología por parte del cliente, datos de eventos de vida del cliente, y demás. Dentro de cada categoría, se establece una lista de los datos específicos que se pueden obtener acerca de una persona. En el ejemplo de la categoría de datos de viajes del cliente, Acxciom podrá determinar información como la aerolínea preferida del cliente, si tienen programas de puntos o millas (y en su caso, cuantos puntos o millas tienen), si prefieren leer, dormir, o ver películas durante un vuelo, y la frecuencia con la que viajan. En la categoría de datos de características individuales del cliente, la empresa podrá determinar datos como el aumento de los lentes de ver de un cliente, sus afiliaciones políticas, e inclusive hasta el “inferred household rank”, es decir, el poder de mando que se infiere que tiene el cliente dentro de su núcleo familiar. El catálogo también proporciona una guía que ayuda a las marcas a determinar que categorías de datos les pueden ser relevantes con base en su giro.

Finalmente, el catálogo habla de “Personicx”, el programa de segmentación desarrollado por Acxciom que busca atribuir los datos mencionados anteriormente, a un grupo de clientes determinados. En la semblanza de Personicx, se revela que la empresa desarrolló 70 segmentos representativos de grupos de personas, y 21 segmentos que representan etapas

de la vida en las cuales se pueden encontrar esas personas. Acxiom plantea que mediante sus estudios y recolección de datos existen 70 tipos de clientes específicos, y se entra en detalle en cuanto a cómo es cada uno. De igual manera, a cada grupo se le atribuye un nombre diferente, por ejemplo el grupo 5, denominado “Sitting Pretty”. Se menciona que el cliente perteneciente al grupo “Sitting Pretty” es aquel que está a punto de jubilarse, cómodo con sus ahorros y con hijos mayores que ya no viven en casa. Se menciona que el cliente “Sitting Pretty” tiende a vivir una vida de lujos, y vivir en los suburbios. Datos de viajes del cliente pudieran delatar a un adulto perteneciente al grupo 5. Por otro lado, hay grupos como el 59 que representan los “Mobile Mixers”. Los “Mobile Mixers” se describen como grupos de personas de bajos ingresos que tienden a mudarse mucho por temas de rentas. Se establece que estas personas suelen vivir en ciudades grandes y que muchas veces son personas sin licenciatura. Como estas categorías, hay 68 más, y todas son altamente específicas. Mediante este tipo de prácticas de profiling, las empresas podrán utilizar los datos de sus clientes para embonarlos dentro de cierto grupo, y así, entender y predecir sus comportamientos.

Con el tiempo, las prácticas de profiling han evolucionado, convirtiendo a los posibles perfiles en unos cada vez más específicos y acertados- especialmente ya que nuestras huellas digitales solo van creciendo con el tiempo. Estos programas que antes podrían determinar los gustos personales de un usuario, hoy en día podrán ser utilizados para determinar condiciones de salud subyacentes, estrategias de planificación familiar, y otros temas potencialmente sensibles.

2. CONCEPTO DE DATOS PERSONALES

En este subtítulo, se llevará a cabo una exposición del concepto de los datos personales desde una óptica jurídica. Para lograr lo último, se expondrán tres subtemas distintos. Primero, se abordará la regulación de los datos personales tanto a nivel nacional, como internacional. Posteriormente, compararemos los tipos de datos personales, así como los avisos de privacidad que podrán, en su caso, regular su almacenamiento.

2.1 REGULACIÓN DE LOS DATOS PERSONALES

La Ley Federal de Protección de Datos Personales en Posesión de los Sujetos Obligados, así como la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (también conocida como la LFPDPPP, por sus siglas) son las legislaciones aplicables en México en materia de privacidad de datos. Estas leyes secundarias son reglamentarias de distintos artículos de la Constitución, incluyendo primordialmente al artículo 6, y al 16. Es decir, la protección de datos personales no emana de la LFPDPPP, si no, de la misma Constitución. En su artículo 6-A fracción 2, se denota lo siguiente:

“Artículo 6o. La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida privada o los derechos de terceros, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.

Toda persona tiene derecho al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión.

El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios.

Para efectos de lo dispuesto en el presente artículo se observará lo siguiente:

A. Para el ejercicio del derecho de acceso a la información, la Federación y las entidades federativas, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:

....

II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.”

Este es un artículo extenso que comprende muchas ideas, pero para efectos de esta investigación, sirve para sentar las bases de dos elementos importantes. El primero, es que tanto la manifestación de las ideas, como el acceso a la información, a pesar de ser derechos constitucionales, tienen sus límites. Aquí se da a entender que la vida privada, así como los datos personales son derechos que prevalecen cuando se ponderan contra el derecho a la manifestación de ideas y/o el acceso a la información. Esta interpretación de la norma es avalada también por la Suprema Corte de Justicia de la Nación en el Amparo en revisión 168/2011, mismo que se transcribe a continuación:

“INFORMACIÓN CONFIDENCIAL. LÍMITE AL DERECHO DE ACCESO A LA INFORMACIÓN (LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL). Las fracciones I y II del segundo párrafo del artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, establecen que el derecho de acceso a la información puede limitarse en virtud del interés público y de la vida privada y los datos personales. Dichas fracciones sólo enuncian los fines constitucionalmente válidos o legítimos para establecer limitaciones al citado derecho, sin embargo, ambas remiten a la legislación secundaria para el desarrollo de los supuestos específicos en que procedan las excepciones que busquen proteger los bienes constitucionales enunciados como límites al derecho de acceso a la información. Así, en cumplimiento al mandato constitucional, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental establece dos criterios bajo los cuales la información podrá clasificarse y, con ello, limitar el acceso de los particulares a la misma: el de información confidencial y el de información reservada. En lo que respecta al límite previsto en la Constitución, referente a la vida privada y los datos personales, el artículo 18 de la ley estableció como criterio de clasificación el de información confidencial, el cual restringe el acceso a la información que contenga datos personales que requieran el consentimiento de los individuos para su difusión, distribución o comercialización. Lo anterior también tiene un sustento constitucional en lo dispuesto en el segundo párrafo del artículo 16 constitucional, el cual reconoce que el derecho a la protección de datos personales —así como al acceso, rectificación y cancelación de los mismos— debe ser tutelado por regla general, salvo los casos excepcionales que se prevean en la legislación secundaria; así como en la fracción V, del apartado C, del artículo 20 constitucional, que protege la identidad y datos personales de las víctimas y ofendidos que sean parte en procedimientos penales. Así pues, existe un derecho de acceso a la información pública que rige como regla general, aunque limitado, en forma también genérica, por el derecho a la protección de datos personales. Por lo anterior, el acceso público —para todas las personas independientemente del interés que pudieren tener— a los datos personales distintos a los del propio solicitante de información sólo procede en ciertos supuestos, reconocidos expresamente por las leyes respectivas. Adicionalmente, la información confidencial puede dar lugar a la clasificación de un documento en su totalidad o de ciertas partes o pasajes del mismo, pues puede darse el caso de un documento público que sólo en una sección contenga datos confidenciales. Por último, y conforme a lo dispuesto en el artículo 21 de la ley, la restricción de acceso a la información confidencial no es absoluta, pues puede permitirse su difusión, distribución o comercialización si se obtiene el consentimiento expreso de la persona a que haga referencia la información.”¹⁸

La tesis citada sirve para confirmar la interpretación sistemática de lo establecido en el artículo 6-A fracción 2 de la Constitución. Misma interpretación, que mientras reconoce al acceso a la información como un derecho que debe ser salvaguardado, también supone que este no se encuentra en un plano de igualdad al ponderarlo contra la protección de datos personales. Esto último, por consecuencia de que la protección de datos personales se comprende como una parte íntegra del derecho a la vida privada, que es un derecho humano reconocido a nivel internacional.

¹⁸Tesis: 1a. VII/2012, Registro: 2000233. Semanario Judicial de la Federación y su Gaceta, Décima Época, Libro V, febrero de 2012, Tomo 1, Primera Sala, p. 655, Disponible en: https://www.scjn.gob.mx/Transparencia/Documents/CriteriosPJF/Tesis_tematica_Datos_Personales.pdf (Consulta: Septiembre 2024)

Asimismo, el segundo elemento que se resalta tanto en el artículo 6to constitucional, como en la tesis citada, es la remisión a las leyes generales en materia de protección de datos personales con respecto de las indicaciones específicas de sus lineamientos. Es decir, la última oración del artículo 6to constitucional sirve como una especie de “llamada a acción” para el legislador de elaborar leyes generales que sirvan para salvaguardar este derecho. Hasta cierto punto, la Constitución busca “delegar” la responsabilidad de elaborar ordenes normativos que rigen los datos personales- como lo es en el caso de la LFPDPPP y la LFPDPPP, así como la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y otras normativas relevantes.

De igual manera, se vuelve a ilustrar la importancia de la protección de datos personales en el artículo 16 constitucional, donde se redacta lo siguiente:

“Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.”

De lo anterior, podemos comprender que los datos personales son elementos que no solo son reconocidos constitucionalmente, si no, constituyen un derecho que se debe proteger.

Ahora bien, si tomamos en cuenta el alcance de la obtención de datos personales en el contexto histórico actual, sería adecuado considerar que hay cierta invasión a la privacidad de los usuarios del internet. Como fue mencionado en el desglose de las prácticas de Acxiom, los datos captados pueden variar desde lo más banal, hasta a lo más personal. Dicho esto, se puede interpretar que el artículo constitucional vela por los datos personales, porque al protegerlos se protege a la privacidad del gobernado. El derecho a la vida privada es un derecho humano, mismo que se reconoce por la Declaración Universal de Derechos Humanos en su artículo 12. Se versa como sigue;

“Artículo 12 Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.”

Ahora bien, si no existe como tal una definición universal de “vida privada” podemos concluir que la protección de datos personales es un derecho reconocido por la constitución, con bases en el derecho humano a la vida privada.

Por otro lado, valdría la pena también analizar la normativa en materia de protección de datos personales en la Unión Europea. El enfoque central será en el GDPR, ya que este es el ejemplo mundial en materia de privacidad de datos, y sobre todo, hasta cierto punto el “blueprint” para muchas de las disposiciones que se podrán observar en la legislación mexicana en materia de privacidad de datos.

El General Data Protection Regulation (el Reglamento General de Protección de Datos) o “GDPR”, esta es una regulación emitida por la Unión Europea que, como menciona su nombre, se dedica a reglamentar la protección de datos. Esta legislación promulgada en el 2016 rige a todas las empresas que procesan, almacenan o tratan datos personales de usuarios de la Unión Europea. Al ser uno de los primeros reglamentos que ponía en riesgo las operaciones de las empresas tecnológicas en 28 países, los lineamientos establecidos en el GDPR incentivaron a las mismas a mejorar sus prácticas relativas a los datos personales. Es por esto, que se considera que este reglamento es el ejemplo a seguir para muchas leyes y códigos (en materia de protección de datos personales) que aún están siendo desarrollados a través del mundo. ¹⁹

En términos simples, el GDPR surge para establecer los lineamientos para el procesamiento de datos personales, así como para regir el movimiento “libre” de los mismos. Al igual que en México, en el GDPR se reconoce que la protección de los datos personales de los particulares es un derecho fundamental que debe ser salvaguardado. Sin embargo, a

¹⁹Wolflord, Ben “What is GDPR, the EU’s new data protection law?”. Suiza, 2020. Disponible en línea: [GDPR.EU < https://gdpr.eu/what-is-gdpr/>](https://gdpr.eu/what-is-gdpr/) (Consulta: Marzo 2024);

diferencia de la legislación Mexicana, también se da a entender que el procesamiento de datos es indispensable para el acceso a la información, y también para la innovación, por lo cual se busca encontrar armonía entre ambas ideas. Esta concepción será analizada más adelante en este capítulo.

Para entrar en contexto con respecto de los alcances de esta regulación, es importante comprender su ámbito de aplicación en términos territoriales. Se menciona en el GDPR que los lineamientos establecidos deberán ser observados por a) las personas morales que compran, venden, o den tratamiento a los datos personales dentro del territorio de la Unión Europea; b) las personas morales que compran, venden, o den tratamiento a datos personales de sujetos que se encuentren dentro de la Unión Europea o; c) cualquiera que compra, venda, o de tratamiento a datos personales cuando se encuentren en territorios ajenos a la Unión Europea, siempre y cuando ese territorio haya adaptado los lineamientos del GDPR en virtud del derecho internacional público. También, se resalta que es una ley que se fija únicamente en proteger a las personas físicas, y no morales.

Al igual que en la LFPDPPP, el GDPR establece que hay ciertos límites cuando se refiere a proteger los datos personales. Por ejemplo, en su artículo 16, la normativa establece que el procesamiento de datos en situaciones de seguridad nacional queda excluido de los lineamientos que se establecen posteriormente. Así como esta diferencia, existen muchas más entre el GDPR en la Unión Europea y la LFPDPPP en México. Es por esto, que a continuación, se lleva a cabo un desglose de algunas de las principales diferencias que se podrán notar entre ambas legislaciones cuando se trata de proteger datos personales.

Tema a tratar	Planteamientos en GDPR	Planteamientos en LFPDPPP
Protección de datos personales como derecho fundamental	El GDPR refiere a la protección de datos personales como un derecho fundamental en distintas	No existe dentro de la LFPDPPP alguna disposición que establezca a la protección de datos

	ocasiones a través de sus disposiciones. Sin embargo, explica más a fondo los alcances y los límites del derecho en su artículo 4 donde se dispone lo siguiente: “The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.”	personales como un derecho fundamental, ya que es una ley secundaria, cuya función es complementar a lo establecido por la Constitución. Sin embargo, sabemos que tanto en el artículo 6 como en el 16 constitucional se reconoce a la protección de datos personales como derecho fundamental. Por otro lado, a diferencia de lo planteado en el GDPR, no se establece en el orden normativo la jerarquía que se deberá de observar con respecto de la protección del derecho mencionado. No obstante, si existen tesis emitidas tanto por los tribunales colegiados de circuito como por la misma Suprema Corte de Justicia de la Nación donde se lleva a cabo la ponderación de derechos que podrán contraponerse con el derecho a la protección de datos personales. A pesar de que no existe un criterio generalizado en relación al tema a tratar, si existen casos, como en el Amparo en revisión 168/2011, donde se resuelve que el derecho a la vida
--	---	---

	Este artículo da a entender que, a diferencia de México, la importancia del derecho a protección de datos personales solamente podrá ser determinada cuando se pondera contra otros derechos fundamentales que podrán posicionarse en contra del primero. Es así que se da a entender que este derecho solamente podrá ser protegido cuando no se contraponga con distintos derechos que se mencionan posteriormente en el artículo, como el derecho al acceso a la información.	privada va por encima del derecho al acceso a la información.
Tratamiento de datos de menores de edad	En el caso del GDPR, existen también disposiciones donde se habla acerca del especial cuidado que se habrá de tener en el caso de comprar, vender o dar tratamiento a datos cuyos titulares son menores de edad. Tan es así, que se ofrece una disposición en su artículo 38 donde se menciona lo siguiente: “Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their	Ahora bien, por más que no se establezca en ninguna disposición de la LFPDPPP que los “niños” gozarán de una especial protección de datos personales, sabemos que en el derecho mexicano existe el principio de interés superior del menor, mismo principio que rige todas las ramas del derecho- donde se busca velar por los intereses de los menores de edad ante cualquier situación.²⁰

²⁰ Ramírez Bañuelos, José Francisco, “Pautas Para la Aplicación del Principio del Interés Superior del Niño en México”. México, Noviembre 14 2021. Disponible en línea: IUS Doctrina Volumen 14, <file:///Users/anamoncayo/Downloads/48953-Texto%20del%20art%C3%ADculo-197271-1-10-20211101.pdf>(Consulta: Septiembre 2024)> (Consulta, Septiembre 2024)

	rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.” En el artículo citado, se habla de la protección especial que se deberá de otorgar a los niños (no se especifica a qué edad se siguen considerando como tal) bajo la premisa de que por su niñez, no comprenden los riesgos del procesamiento de su información. De igual manera, refiere a el tipo de tratamiento que se da a los datos personales de los niños refiriendo meramente a temas publicitarios. Es así, que se sugiere que el tratamiento de datos de los niños solo podrá	De modo similar, en México existe la figura de la capacidad legal, que habla de la posibilidad que tiene una persona física de contraer obligaciones, como lo es en el caso de los contratos. Ahora bien, por regla general, los menores de edad no tienen capacidad legal, por lo mismo que se menciona en el artículo 38 del GDPR- los “niños” en muchas ocasiones no comprenden los riesgos y las consecuencias de contraer obligaciones, imposibilitándolos de otorgar un consentimiento sin vicios.
--	--	---

	llevarse a cabo mediante servicios dirigidos hacia los mismos. Finalmente, se expone que a pesar de haber planteado que los niños no tienen conocimiento suficiente para conocer los riesgos del procesamiento de sus datos, no será necesario que los padres de familia den consentimiento para permitir el mismo.	
--	---	--

2.2 TIPOS DE DATOS PERSONALES

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares define a los datos personales como “cualquier información concerniente a una persona física identificada o identificable”²¹ Teniendo esto en mente, podemos asumir que cualquier información que puede concernir a una persona física puede comprender un sinnúmero de cosas, desde lo más vago hasta lo más específico. Bajo esta definición, un dato personal puede comprender algo básico como el género de una persona, o algo más sensible como la ruta exacta que toma esa misma persona para llegar al trabajo en determinada fecha. Es por esto, que los datos personales caben dentro de distintas categorías, mismas que se desglosarán a continuación.

Los primeros tipos de datos personales que se mencionaran son aquellos que determinan una demografía. Estos datos se conforman de factores generales como nombre, edad, domicilio, escolaridad, estado civil, y demás. Los datos demográficos pueden ser

²¹ Davara, Isabel. “**Diccionario de Protección de Datos Personales: Conceptos Fundamentales**. México: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Primera ed. Noviembre del 2019.

obtenidos más fácilmente por el uso de redes sociales, mientras los datos sensibles pueden ser más privados o más bien, ser más difíciles de acceder. Es decir, independiente de la participación en redes sociales de un individuo, esta información es accesible para el público general, y las más de las veces es proporcionada directamente por el titular de la información.

De igual manera, existen los datos sensibles. Estos son datos personales que pasan a ser más privados que los demás por su naturaleza. El artículo 3 fracción V de la LFPDPPP los define como;

“Datos personales sensibles: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.”

En el artículo anterior, se desglosan dos factores que pueden constituir un dato sensible. El primero siendo que el dato sea de índole “íntimo” (aunque no se define el término), y el segundo siendo que el conocimiento del dato pueda causar perjuicio a su titular. Partiendo de una interpretación literal de esta oración, podemos ver que los últimos factores no tendrían que manifestarse conjuntamente para ser considerados como un dato sensible. Es por esto, que esta definición proporcionada es ambigua en el sentido de que no se menciona una concepción de lo que se considera “íntimo”. La deficiencia en esta definición también radica en el hecho de que, el uso indebido de cualquier dato (inclusive los de acceso público) pudieran causar perjuicio a su titular. Sin embargo, el artículo continúa con un enlistado de algunos tipos de datos que pudieran caer en alguno de los supuestos mencionados. Entre ellos, datos relevantes a la raza, etnia, estado de salud, genética, creencias, afiliaciones, opiniones, y preferencias sexuales del titular. Partiendo de estos ejemplos, se concreta una definición más clara y concisa de los tipos de datos que se pueden considerar sensibles.

Comprendiendo la diferencia entre los datos demográficos y sensibles, es importante hablar acerca de los tipos de datos se tienden a obtener mediante el “data broking”. En una encuesta realizada por el comité de comercio, ciencia y transporte del senado de Estados Unidos, se determinaron una serie de factores que son utilizados para

segmentar clientes. Para realizar esta encuesta, el comité entró en contacto con 9 empresas cuyos giros consisten de la compra y venta de datos personales.²²

Aquí, se realizaron una serie de preguntas a cada una de las empresas con la finalidad de dar a comprender el trabajo de los “data brokers” ante el senado, y en turno, crear legislación relevante. Se reveló que la información que tiende a ser recolectada por los data brokers puede ser dividida en 5 categorías. La primera es información de transacciones y compras por parte de los clientes. Esto comprende las fechas en las que se realizó un pago, la modalidad, y la frecuencia con cuál se realizan distintos pagos por distintos clientes. La segunda, es información relevante a los métodos de pago de los clientes. Esto incluye información bancaria acerca de las cuentas de los clientes, así como su información de tarjeta de crédito y/o débito. La tercera, por alguna razón, es la compra y venta de automóviles en las que ha participado el cliente. Se guardan datos con respecto de los automóviles que conducen los clientes, así como sus preferencias en esa misma cuestión (si prefieren autos nuevos o usados, que marcas les gustan, etc.). La cuarta se enfoca en padecimientos médicos de los clientes (pueden ser padecimientos diagnosticados o no, es decir, la empresa puede predecir el padecimiento antes que el mismo cliente). Se indica que había empresas encuestadas que reportaban ofrecer listas de personas con enfermedades como cáncer, alzhéimer, diabetes, y depresión a terceros. Por último, la quinta categoría comprende el uso de redes sociales. Esta información puede variar desde el contenido publicado por un usuario y sus seguidores, hasta a los videos que ven en Youtube.

Los últimos son solo 5 tipos de datos que comúnmente fueron recolectados por los data brokers que formaron parte de la encuesta, pero estos no son los únicos. Quienes condujeron la encuesta encontraron que había empresas que almacenaban datos más específicos, y difíciles de obtener. Se reportó se buscaba información como el número de visitas al ginecólogo que habían tenido ciertas clientes y la cantidad de whiskeys que se habían tomado los clientes en el último mes.²³ Este ejemplo, es solamente uno de muchos

²² Estas fueron las empresas: Spokeo, Datalogix, TransUnion, Rapleaf, Equifax, Reed Elsevier, Experion, Acxiom, y Epsilon).

²³ Office of Oversight and Investigations Majority Staff. **A Review of the Data Broker Industry: Collection, Use and Sale of Consumer Data for Marketing Purposes**. 18 de diciembre del 2013. p. 23. Disponible en línea: Committee on Commerce, Science, and

cuando se habla acerca del tratamiento de nuestros datos para en turno, convertirlos en datos sensibles.

2.3 AVISOS DE PRIVACIDAD Y DATOS PERSONALES

En seguimiento a la comprensión de la venta de datos personales, es importante primero entrar en contexto con respecto de cuáles son los datos personales que estamos compartiendo y por qué medios los compartimos. El objetivo de este apartado más que nada es dar a entender que la venta de datos no se limita a la información que compartimos a nuestras redes sociales, sino, que también comprende nuestros hábitos, nuestras rutas al transitar, e inclusive información médica y bancaria.

En la Guía para la elaboración del Aviso de Privacidad publicado por el INAI, se describen los Avisos de Privacidad como:

“Documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular; previo al tratamiento de sus datos personales. El aviso de privacidad tiene por objeto establecer y delimitar los alcances y condiciones generales del tratamiento, así como informar a las personas titulares, a fin de que estén en posibilidad de tomar decisiones informadas sobre el uso de sus datos personales, de mantener el control y disposición sobre ellos; asimismo, permite al responsable transparentar dicho tratamiento, y con ello fortalecer el nivel de confianza de las personas titulares.”²⁴

En ejemplos prácticos, el aviso de privacidad tiende a manifestarse como un “pop up” o una ventanilla que aparece a la hora de navegar alguna página de internet o red social. Como menciona la definición proporcionada por el INAI, son documentos cuya responsabilidad de compartir recae sobre los responsables del tratamiento de datos personales- es decir, la misma plataforma que se está utilizando. Los avisos de privacidad

Transportation. United States Senate.<<https://www.commerce.senate.gov/services/files/0d2b3642-6221-4888-a631-08f2f255b577> > (Consulta: Marzo 2024)

²⁴ Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales **“Guía para la elaboración del Aviso de Privacidad”**. Primera Edición. Mayo, 2022. Disponible en línea: INAI <https://home.inai.org.mx/wp-content/uploads/GuiaElaboracion_AvisoPrivacidad_Area_RH.pdf>(Consulta: Agosto 2024)

NO son de naturaleza optativa para quienes tratan datos, ya que la LFPDPPP establece en su artículo 15 la obligatoriedad de estos.

“Artículo 15.- El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.”

Posteriormente en la ley citada, se habla acerca de ciertos lineamientos que deberán seguir los avisos de privacidad para ser totalmente transparentes con respecto de su uso de datos. En su artículo 17, se menciona lo siguiente;

“Artículo 17.- El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología, de la siguiente manera:

Cuando los datos personales hayan sido obtenidos personalmente del titular, el aviso de privacidad deberá ser facilitado en el momento en que se recaba el dato de forma clara y fehaciente, a través de los formatos por los que se recaban, salvo que se hubiera facilitado el aviso con anterioridad, y

Cuando los datos personales sean obtenidos directamente del titular por cualquier medio electrónico, óptico, sonoro, visual, o a través de cualquier otra tecnología, el responsable deberá proporcionar al titular de manera inmediata, al menos la información a que se refiere las fracciones I y II del artículo anterior, así como proveer los mecanismos para que el titular conozca el texto completo del aviso de privacidad.”

Este artículo resulta pertinente al mencionar críticas hacia la forma en que se regula el tratamiento de datos personales- de igual manera va de la mano con la definición de aviso de privacidad que se analiza en el presente capítulo. Los avisos de privacidad son eso- un aviso solamente. Son meramente herramientas utilizadas para facilitar la transparencia con respecto de las prácticas de las empresas tecnológicas, que sirven para enunciar (aunque sea en términos sumamente vagos) las prácticas que se llevan a cabo con datos ajenos. Pero como se menciona en el artículo 17, este aviso no se tiene que dar previo a la recolección de datos, si no, se da inmediatamente cuando ya fue captada la información necesaria. El defecto o la ineficiencia del aviso de privacidad recae en su misma naturaleza- tener consciencia de que están vulnerando un derecho humano no resulta en la protección de este.

Es notorio, que los avisos de privacidad, aunque sirvan como medidas preventivas, no sirven para verdaderamente prevenir ningún daño que se pudiera ocasionar a la hora de comprar, vender o dar tratamiento a los datos personales.

CAPÍTULO II

CASOS TRASCENDENTALES

Este capítulo examina los derechos humanos que se pueden ver afectados a través de la vigilancia cibernética y la venta de datos personales. Para ilustrar las esferas jurídicas que se vulneran a la hora de compartir información personal, se analizarán 2 casos que han sido expuestos ante tribunales en los últimos años. Los casos concretos a tratar serán el caso de Google contra el estado de California, y el caso de la aplicación Flo.

1. GOOGLE VS. ESTADO DE CALIFORNIA.

A lo largo de los últimos años, la empresa Google (así como muchas otras empresas tecnológicas) ha sido sujeto de una serie de litigios por cuestiones de violaciones en distintos temas; desde antitrust hasta ciber seguridad.

En razón de la información presentada a lo largo de esta investigación, resulta relevante mencionar las demandas presentadas en contra de Google por razón de protección de datos personales. En el 2022, se reporta que 40 estados norteamericanos promovieron demandas en contra de la empresa, mismas que resultaron en acuerdos reparatorios con un valor de más de \$350 millones de dólares.²⁵

²⁵ Kang, Cecilia. “**Google reaches \$391.5 million settlement over privacy practices**”. Estados Unidos: Noviembre 14, 2022. Disponible en línea: The New York Times, Tech <<https://www.nytimes.com/2022/11/14/technology/google-privacy-settlement.html>> (Consulta: Marzo 2024)

1.1 ANTECEDENTES DEL CASO.

El caso concreto versa sobre las faltas cometidas por Google en contra de sus usuarios, al utilizar su ubicación geográfica a tiempo real en contra de su voluntad. Como hemos visto, cada vez hay más conciencia acerca del almacenamiento de nuestros datos. A la par, cada vez hay más marcos regulatorios que obligan a las empresas a darle la opción a sus usuarios de “opt out” de compartir ciertos datos. En cumplimiento de este marco, empresas como Google se vieron obligadas a permitir que sus usuarios pudieran inhabilitar ciertas funciones que facilitaban rastreos que se pudieran ser considerar como invasivos.

La implementación de esta medida es deficiente por su naturaleza, ya que la transparencia en cuanto a las prácticas invasivas está condicionada a la disposición del usuario de leer términos y condiciones que pueden ser largas y difíciles de comprender. Aun así, habían usuarios quienes optaron por no permitir el acceso a información sensible, incluyendo la ubicación geográfica a tiempo real.

Sin embargo, una investigación publicada por el noticiero Associated Press determinó que Google seguía recolectando datos de rastreo de sus usuarios a pesar de que estos hubieran optado por no compartir esa información.²⁶ Dentro de esta investigación realizada por estudiantes de la Universidad de Princeton, se determinó que esta práctica estaba siendo utilizada por Google desde el 2014.

Como sabremos, “Google” comprende no solamente el navegador de internet, sino, una serie de aplicaciones como Gmail y Google Maps. En el caso de Google Maps, es indispensable el uso de ubicaciones, ya que la aplicación tiene por objeto llevar al usuario de un punto a otro, proporcionando las rutas adecuadas. Sin embargo, en aplicaciones como esta, los usuarios podían prender o apagar la opción de “historial de ubicación”. El historial

²⁶ Nakashima, Ryan. “Google Tracks your Movements, Like it or Not”. Estados Unidos: Agosto 13, 2018. Disponible en línea: Associated Press <<https://apnews.com/article/828aefab64d4411bac257a07c1af0ecb>> (Consulta: Marzo 2024)

de ubicación permite a Google Maps a almacenar las rutas que fueron tomadas en ocasiones anteriores, así como vender esta información a terceras partes.

Uno de los problemas, fue que, a pesar de elegir la opción de apagar el historial de ubicación, este seguía siendo recolectado por Google, quien había establecido en sus términos y condiciones que esto no pasaría. De igual manera, se determinó que la recolección de ubicación no solamente era utilizada por Google Maps (donde es necesario). Los investigadores de Princeton descubrieron que usuarios que utilizaban otras aplicaciones como Gmail, o inclusive el mismo buscador de Google, podrían ser rastreados a tiempo real cada vez que abrían la página. Este descubrimiento fue grave, ya que se expone que la empresa hace caso omiso a las necesidades de sus usuarios en cuanto a su ciberseguridad. De igual manera, la investigación puso en duda la veracidad de lo establecido en los términos y condiciones de todas las empresas tecnológicas. El artículo publicado por Associated Press planteó dudas en la mente de muchos, ¿qué tantos de nuestros datos sensibles están siendo utilizados por empresas tecnológicas? ¿Qué tan reales son los términos y condiciones a los que accedemos los usuarios?

A luz de lo anterior, el fiscal general del estado de California en estados unidos decidió demandar a Google por sus prácticas violatorias de privacidad. Esta demanda inició un efecto dominó, por el cual posteriormente un total de 40 estados estadounidenses se unieron en contra de la empresa tecnológica. Las demandas alegan que la empresa estableció afirmaciones totalmente falsas, engañando a sus usuarios. La consecuencia para Google resultó en no solamente pagar arriba de \$90 millones de dólares a la fiscalía del estado de California, sino también en una serie de medidas preventivas que deberán de ser cumplidas por la empresa.

Las medidas (mismas que son expresadas a través de un mandato judicial con 48 disposiciones) varían desde auditorías por asesores independientes, hasta reformas a las

políticas de la empresa.²⁷ Entre estas últimas, se observa que muchas de las obligaciones a las que se somete Google hacen énfasis en la transparencia y accesibilidad total que deberán de tener sus términos y condiciones. Tan es así, que se dicta el lenguaje específico que se deberá de utilizar para divulgar información relevante a la privacidad de datos. El lenguaje fue diseñado por la autoridad para ser entendible por todos los usuarios. También, se ordena a notificar al usuario mediante “pop-ups” cada vez que se utilizará su ubicación, a su vez proporcionando una liga para una página que expone todos los lineamientos de privacidad de datos. Dentro de la página, deberá de haber transparencia total con respecto de los alcances de la información que es recolectada por Google, así como los motivos por los cuales esa información se comparte con terceras partes. Finalmente, se exige que Google solamente utilice datos de ubicación de los usuarios que han cedido mediante “consentimiento expreso afirmativo”.

1.2 ANÁLISIS JURÍDICO.

La litis de en el caso de Google vs. el Estado de California, es consistente en determinar si Google violó la privacidad de sus usuarios al utilizar los datos sensibles de sus usuarios a través de prácticas engañosas.

En la queja proporcionada por la Corte Superior del Estado de California, se desglosan los hechos que ocasionaron la demanda en contra de Google. En el desglose, se explican las razones por las cuales los avisos de privacidad de Google fueron deficientes para efectos de recibir un “consentimiento expreso” por parte de los usuarios para ceder sus datos sensibles. En el subtítulo “Defendants Business Acts and Practices” (“Actos de Negocios y Prácticas del Acusado” en español), se reitera lo siguiente:

²⁷ (Proposed) Final Judgement and Permanent Injunction, **The People of the State of California v. Google, LLC**. Supreme Court of the State of California for the County of Santa Clara, Estados Unidos: Septiembre 2023. Disponible en línea: <<https://oag.ca.gov/system/files/attachments/press-docs/Google%20Proposed%20Order%20FINAL%20%283%29.pdf>> (Consulta: Marzo 2024)

“As discussed further below, many users did not know of or understand Google’s Location History and Web & App Activity settings, yet had unwittingly enabled them due to Google’s deceptive disclosures, thereby allowing Google to track their precise location. In addition, Google misrepresented that when users disabled Ads Personalization it would stop using the user’s location to target advertisements to those users, when in fact it continued to do so.

(Como se discute posteriormente, muchos usuarios no sabían de o comprendían los ajustes de Historial de Ubicación y Actividad de Aplicación/Web de Google, y aún así las habían inconscientemente habilitado gracias a las divulgaciones engañosas de Google, por ende permitiendo a Google a rastrear su ubicación precisa. Además, Google tergiversó su acepción de que cuando los usuarios inhabilitaran la personalización de anuncios que dejaría de utilizar la ubicación del usuario para apuntar anuncios a los mismos, cuando de hecho, lo seguían haciendo). ”²⁸

Tomando en cuenta la acepción anterior, sabemos que el problema jurídico no recae en el uso de datos sensibles, si no, en el “método” para conseguir el consentimiento del usuario, y en el incumplimiento de lo establecido por el aviso de privacidad (al hacer pensar a los usuarios que tenían la opción de optar por no compartir sus datos, cuando en realidad, no la tenían).

De igual manera, el problema crece, ya que posteriormente en la queja, se establece lo siguiente:

*“Location History gives Google detailed insights into people’s whereabouts and activities. Google can track when users arrive at and leave a location. Location History collects and stores such records about each person every single day. When a user creates a Google account, the Location History setting is supposedly off by default; however, from 2014 to 2018, Google showed users deceptive prompts when they used certain Google apps to mislead users into unwittingly enabling Location History. For example, when using Google Maps, Google showed users a pop-up that asked if the person wished to “[e]nhance [their] Google Maps experience” because “Google needs to periodically store your location to improve your search suggestions, route recommendations and more.” However, **by enabling this “enhancement,” the user unknowingly turned on Location History, which allowed Google to collect and store the user’s location accountwide—even outside Maps.** By simply clicking on the button labelled “Yes, I’m in” within Google Maps, users were actually consenting to the collection and use of their location data 24/7 by Google. **Defendant also failed to disclose the material fact that it was also using the location data for the wholly unrelated purpose of profiling the user for advertising purposes.**”²⁹*

(Historial de ubicación le otorga a Google información detallada acerca de las actividades y los paraderos de las personas. Google puede rastrear cuando sus usuarios van y vienen de cualquier ubicación. Historial de ubicación colecciona y almacena dichos records acerca de cada persona todos

²⁸ Superior Court of the State of California for the County of Santa Clara. **THE PEOPLE OF THE STATE OF CALIFORNIA VS. GOOGLE, LLC.** Complaint for Injunction, Civil Penalties, and Other Equitable Relief. Case No. 23CV422424. County of Santa Clara: September 14th, 2023. Disponible en línea: <https://oag.ca.gov/system/files/attachments/pressdocs/Filed%20stamped%20Google%20Complaint.pdf>

²⁹ Loc. Cit.

los días. Cuando un usuario crea una cuenta de Google, el ajuste de historial de ubicación supone estar inhabilitado por default. Sin embargo, del 2014-2018, Google le mostró a sus usuarios indicaciones engañosas cuando usaban ciertas aplicaciones de Google para engañar a sus usuarios a inconscientemente habilitar su historial de ubicación. Por ejemplo, al utilizar “Google Maps”, Google utilizaba un “pop-up” para preguntar si la persona quisiera “mejorar su experiencia de Google Maps”, porque “Google necesita periódicamente almacenar tu ubicación para mejorar tus sugerencias de búsqueda, recomendaciones de ruta, y demás.” Sin embargo, al habilitar esta “mejora”, el usuario sin saber estaba habilitando su historial de ubicación, lo cual permitió que Google coleccionara y almacenara la ubicación del usuario a través de todas sus plataformas, inclusive aquellas que no fueran Google Maps. Al simplemente presionar el botón de “Sí, estoy dentro” en Google Maps, los usuarios en realidad estaban consintiendo a la colección y uso de sus datos de ubicación 24/7 por Google. El acusado también falló en mencionar el hecho material de que a parte estaba utilizando dichos datos por motivos totalmente distintos, mismos que consisten en el perfilamiento de usuarios para propósitos publicitarios)³⁰.”

Tomando en cuenta lo subrayado, vemos que aparte de que el consentimiento para compartir datos se ve viciado al ser obtenido mediante redacciones engañosas, el problema también gira en torno al hecho de que los datos sensibles no estaban siendo utilizados para los fines que se mencionaban en el aviso de privacidad. Como vemos en la cita anterior, vemos que a los usuarios les vendían la idea de mejorar sus ajustes de ubicación para mejorar sus experiencias utilizando la aplicación, cuando en realidad, esta información se vendía a terceras partes para que pudieran mejorar sus anuncios publicitarios.

Ahora bien, después de desglosar los hechos, la queja procede a mencionar a las normas que fueron violadas a través de las prácticas llevadas a cabo por Google. Aquí, se remite al “Business and Professions Code Section 17500 ET SEQ” (o el Código de Negocios y Profesiones Sección 17500 en inglés)., específicamente mencionando que se incumple con lo establecido con respecto de publicidad engañosa. Se plantea que Google incumplió con los principios que rigen a estas normas al tener avisos de privacidad que eran engañosos con respecto de sus prácticas de datos personales (específicamente hablando del historial de ubicación, personalización de aplicaciones, y actividad de web y aplicación).

Para concluir, a lo largo de este análisis podemos comprender que Google sí violó la privacidad de sus usuarios a través de 3 prácticas distintas. La primera, fue al crear

³⁰ Esta traducción fue redactada por la autora de esta tesis.

indicaciones engañosas para inducir a sus usuarios al error. Esto es violatorio de la privacidad de sus usuarios, ya que la normativa internacional en materia de privacidad de datos es clara en establecer que, para utilizar datos sensibles de un usuario, el mismo deberá de manifestar su “consentimiento afirmativo expreso”. Por la naturaleza de ese tipo de consentimiento, este no podrá ser otorgado si el usuario (como bien menciona la queja), está inconsciente de lo que está aceptando.

La segunda práctica que fue violatoria de la privacidad de los usuarios fue incumplir con lo establecido en su aviso de privacidad. Esta práctica recae en la misma violación que la pasada, ya que se utilizaron los datos sensibles de los usuarios sin su consentimiento afirmativo expreso, o más bien en contravención del consentimiento del mismo.

Y por último, la tercera práctica violatoria de la privacidad de los usuarios, fue utilizar los datos sensibles para fines distintos a los establecidos en su aviso de privacidad. De nuevo, aunque los usuarios hubieran accedido a compartir su ubicación para mejorar su experiencia utilizando la aplicación “Google Maps”, nunca accedieron a compartir su ubicación al utilizar “Gmail”, por ejemplo. De igual manera, no accedieron a que su ubicación fuera compartido con terceros para fines publicitarios.

En fin, la confirmación de que estas tres prácticas fueron violatorias a la privacidad de datos de los usuarios de Google, fue beneficioso para efectos de la figura del “precedente” que se utiliza en el Common Law. Las acepciones hechas por los tribunales en este caso obligan a las demás plataformas digitales que utilizan datos sensibles, a hacerlo de una manera totalmente transparente, y observando que se lleve a cabo un “consentimiento afirmativo expreso por parte del titular de datos personales.

2 FTC VS. FLO HEALTH, INC.

Al igual que Google, los últimos años han representado grandes retos en materia de privacidad para otras empresas tecnológicas. Flo Health, Inc (“Flo”, un app dedicado a

rastrear ciclos menstruales, enfrentó escrutinio a mano de las autoridades por sus prácticas de venta de datos. A continuación, se abordará el caso del Federal Trade Commission (FTC) contra la empresa Flo.

2.1 ANTECEDENTES DEL CASO.

En el año 2020, la FTC de Estados Unidos emitió una queja con respecto de las prácticas de la empresa Flo. Se alegaba que la empresa (cuyo giro es consiste en el rastreo del ciclo menstrual, así como el registro de síntomas) vendía los datos sensibles de sus usuarias a terceras partes no solamente sin su consentimiento, si no, a pesar de haber establecido en sus términos y condiciones que eso no se haría.³¹

Flo es una aplicación que guarda datos sumamente personales de sus usuarias. Al ser una aplicación que tiene fines de planeación familiar, la aplicación fomenta el registro de todos los eventos que pueden ser relevantes al ciclo menstrual para determinar predicciones más precisas acerca del mismo. La aplicación, aparte de calendarizar las fechas de ovulación y menstruación, incentiva a sus usuarias a incluir información como las fechas donde tuvieron relaciones sexuales, así como incluir si se utilizó algún tipo de método anticonceptivo. También, la aplicación arroja cuestionarios respecto a la salud general de la usuaria bajo la premisa de que esto puede ser información útil para calendarizar el periodo.

Al ser tenedores de información altamente sensible, Flo Health estableció en sus términos y condiciones que jamás venderían la información sensible de sus usuarias a terceras partes. Asimismo, se estableció que la única información que se pudiera compartir sería aquella que pudiera ser utilizada para mejorar el funcionamiento de la aplicación, como fallas reportadas o un conteo de las veces que se borró la aplicación.

³¹ Federal Trade Commission. **Flo Health, Inc. complaint** (2023). [PDF]. <https://www.ftc.gov/system/files/documents/cases/flo_health_complaint.pdf> (Consulta: Marzo 2024)

Sin embargo, en el año 2020, la FTC descubrió que Flo había estado vendiendo los datos sensibles de sus usuarias a por lo menos 5 empresas dedicadas al data brokerage. A la luz de un reportaje publicado por de the Wall Street Journal se descubrió que Google, Facebook, Flurry, Fabric y Appsflyer compraban datos de categoría de salud de Flo. Más allá de esto, se descubrió también que en los contratos celebrados con estas empresas, Flo permitía el uso ilimitado de los datos personales de más de 100 millones de usuarias. Es decir, Flo autorizó que estos datos fueran utilizados para cualquier fin.

Posterior a la emisión de la queja descrita en los incisos anteriores, se llegó a un acuerdo entre la Federal Trade Commission y Flo. A diferencia del caso de Google (que fue desglosado al inicio de este capítulo), el acuerdo establecido no incluía una sanción económica.³² Sin embargo, fue un caso donde se marcó un precedente en cuanto a la privacidad de datos, y las facultades que puede ejercer la FTC para asegurar que las prácticas de las empresas tecnológicas cumplan con los lineamientos de la normativa vigente relevante.

El acuerdo consiste en una serie de disposiciones que serán desglosadas a detalle en el siguiente apartado (el apartado de análisis jurídico). Sin embargo, cabe recalcar que la FTC dictó ciertas acciones que deberían de ser llevadas a cabo por Flo para evitar incurrir en violaciones a futuro. Entre las acciones que destacan, una incluye a la obligación de Flo de notificar a sus usuarias acerca de la violación que fue cometida en su contra al compartir su información sensible sin su consentimiento, así como también hacerlas saber de sus políticas engañosas. De igual manera, la empresa se vio obligada a trabajar con las terceras partes que recibieron los datos sensibles de sus usuarias para lograr borrar toda la información que fue vendida. Finalmente, también se dictaron distintos lineamientos que la empresa debería de seguir para elaborar sus nuevos términos y condiciones con base en la verdad, y no afirmaciones engañosas.

32 Lomas, Natasha. “**Flo gets FTC slap for sharing user data when it promised privacy**”. Estados Unidos: Enero 13, 2021. Disponible en Línea: Tech Crunch <<https://techcrunch.com/2021/01/13/flo-gets-ftc-slap-for-sharing-user-data-when-it-promised-privacy/#:~:text=No%20financial%20penalty%20is%20being,notice%20of%20a%20privacy%20action.>> (Consulta: Mayo 2024)

En términos generales, se puede decir que este caso fue un parteaguas en cuanto a varios temas dentro de la privacidad de datos. Primero, por establecer precedente en materia de la transparencia que se deberá de observar dentro de los términos y condiciones. Segundo, al dar visibilidad a la venta de datos sensibles, inclusive cuando estos incurren en temas de salud.

2.2 ANÁLISIS JURÍDICO.

Esta práctica llevada a cabo por Flo no solamente atentaba en contra de la integridad de sus usuarias, sino también violó los estatutos establecidos por el EU-U.S. Privacy Shield (“Privacy Shield”). El Privacy Shield es un mecanismo que establece los lineamientos de privacidad de datos que deberán de seguir empresas tecnológicas estadounidenses con usuarios en la Unión Europea. Las empresas tecnológicas que quisieran almacenar datos de usuarios de la Unión Europea se vieron obligadas a firmar el Privacy Shield, y acceder a estar en cumplimiento legal con sus términos y condiciones.

En la queja por parte del FTC, se establece que Flo incurrió en violaciones al Privacy Shield al no proporcionarle a sus usuarias una opción de “opt-out” de compartir sus datos personales. También, se violó el principio de “rendición de cuentas en materia de transferencias”, un principio que obliga a los participantes del Privacy Shield a hacerse responsables de limitar el uso de datos que venden a terceras partes. De igual manera, el Privacy Shield obligaba a sus participantes a vender información únicamente con los propósitos establecidos en los términos y condiciones. Como se encontró que la información vendida por Flo fue utilizada por empresas como Flurry con fines de marketing, a pesar de haber establecido que la única venta de datos que se llevaría a cabo sería con fines de mejorar la aplicación. Para terminar con las violaciones cometidas con respecto de los lineamientos del Privacy Shield, se le imputa a Flo la responsabilidad de haber engañado a sus usuarias al

utilizar afirmaciones totalmente falsas con respecto de sus prácticas de privacidad de datos. Finalmente, se establece dentro de la queja que las prácticas realizadas por la empresa también eran violatorias de la 5ta sección del Federal Trade Commission Act. Se menciona la siguiente definición;

Definición en inglés	Definición traducida al Español ³³
“The FTC Act prohibits unfair or deceptive acts or practices. An act or practice may be found to be unfair where it “causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.” A representation, omission, or practice is deceptive if it is likely to mislead a consumer acting reasonably under the circumstances and is likely to affect a consumer’s conduct or decision regarding a product or service. The standards for unfairness and deception are independent of each other. While a specific act or practice may be both unfair and deceptive, an act or practice is prohibited by the FTC Act if it is either unfair or deceptive. Whether an act or practice is unfair or deceptive will in each instance depend upon a careful analysis of	“ El FTC Act prohíbe actos y prácticas engañosas o injustas. Un acto o práctica se podrá considerar injusta cuando esta le ocasiona o podría potencialmente ocasionar un daño sustancial a los consumidores que no es fácilmente evitable por los mismos y no se ve contrarrestada por posibles beneficios para los consumidores o la competencia. Una representación, omisión o practica es engañosa si es probable que esta engañe a un consumidor actuando de manera razonable bajo las circunstancias dadas, y cuando es probable que afecte la conducta o toma de decisiones del consumidor con respecto de un producto o servicio. Los estándares que definen la injusticia y el engaño no son mutuamente exclusivas. Mientras un acto o una práctica específica pueden ser tanto injustas como engañosas, cualquier acto o práctica es

³³ Esta definición fue traducida por la autora de esta tesis.

the facts and circumstances. In analyzing a particular act or practice, the agencies will be guided by the body of law and official interpretations for defining unfair or deceptive acts or practices developed by the courts and the FTC.” ³⁴	prohibida por la FTC si se puede considerar como injusta o engañosa. Determinar si algún acto o práctica se considera como injusta y engañosa dependerá en cada instancia en un análisis cuidadoso de los hechos y circunstancias. En analizar un acto o una práctica en específico, las agencias serán guiadas por el cuerpo normativo y sus interpretaciones oficiales para definir a las prácticas o actos que se consideren injustas o engañosas por las cortes y por la FTC.
--	---

En la definición anterior, hay una serie de puntos claves que resultan importantes para comprender la violación cometida por Flo. Más allá de la venta de los datos, la queja emitida por el FTC establece que lo que estaba verdaderamente mal fue engañar a las usuarias con respecto del uso de sus datos sensibles.

Si bien es claro que sí existe legislación que salvaguarda los derechos de los particulares con respecto de sus datos personales, también es claro la mayoría de esta protección pretende servir solo en función de que el usuario conozca sus derechos, lea un aviso de privacidad, y comprenda lo que estos conllevan. Por más que es obvio que es incorrecto no divulgar los alcances de tus prácticas en cuanto a datos, el problema real es el hecho de que estos datos sí puedan ser vendidos siempre y cuando exista “consentimiento”.

Para concluir, Flo violó la privacidad de sus usuarias a través de tres prácticas distintas (al igual que en el caso de Google que analizamos anteriormente). La primera fue al crear un

³⁴ Federal Trade Commission. “**Developer of popular women's fertility tracking app settles FTC allegations it misled consumers about their data privacy**”. Estados Unidos: Enero 28, 2021. Disponible en línea: FTC, News & Press <<https://www.ftc.gov/news-events/news/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc-allegations-it-misled-consumers-about> > (Consulta: Marzo 2024)

aviso de privacidad no solo engañoso, sino, totalmente fraudulento. Al mentirle a sus usuarias, dándoles un sentido de confianza, las mismas seguían llenando con más y más datos sensibles a la aplicación, ya que fueron llevadas a creer que estos datos nunca serían compartidos. En segundo lugar, Flo violó la privacidad de sus usuarias, al privarlas de la oportunidad de “opt-out” o decidir no compartir sus datos sensibles, en contravención con lo dispuesto en el Privacy Shield. Finalmente, Flo violó la privacidad de sus usuarias al vender sus datos sensibles a terceras partes sin consentimiento, y sin límites con respecto del uso de dichos datos.

CAPÍTULO III

ANÁLISIS DE LAS PROTECCIONES ACTUALES Y SUS INEFICIENCIAS

Habiendo analizado los riesgos en los que incurren los usuarios de plataformas digitales, así como las medidas implementadas por los tribunales de estados unidos para prevenir dichos riesgos, en este capítulo abordaremos las protecciones actuales que existen en México para salvaguardar los datos personales, a la vez identificando los defectos que podrán tener las mismas. Tomando en cuenta el contexto que hasta este punto hemos logrado desglosar, veremos cuales son las precauciones que se han tomado legalmente para ayudar a proteger a los titulares de los derechos y datos personales, para en turno, lograr crear propuestas que pudieran solventar las deficiencias por exponer.

Como se ha expuesto a lo largo de esta investigación, sabemos que estas protecciones no buscan impedir la compra, venta, y tratamiento de datos per se, sino, buscan que los usuarios tengan autonomía sobre sus datos, para así tomar decisiones informadas con respecto de su uso posterior.

1. DE LA DISTINCIÓN DE LOS DATOS SENSIBLES.

Como hemos examinado a lo largo de esta investigación, la protección de datos personales es un derecho que emana del derecho humano a la vida privada. Es un derecho reconocido constitucionalmente, con leyes federales dedicadas a su regulación. Aunado a esto, es un derecho que ha sido ampliamente discutido, regulado y litigado en un marco internacional. Aún así, sigue siendo un término definido tan vagamente, tomando en cuenta los intereses de las personas morales por encima de las físicas. Las incongruencias legales comienzan desde la misma definición del término “Dato Sensible”. Como se dio a entender en el capítulo dedicado a sentar las bases de los datos personales, recordamos también la

definición de los datos sensibles, y los supuestos en los que recae su existencia.³⁵ Ahora bien, si la misma existencia de los datos sensibles implica el posible perjuicio en el que se puede incurrir al divulgarlos, es importante regularlos de una manera distinta a los demás datos. Es por esto que en el artículo 9 y 10 de la LFPDPPP establecen las reglas que se deberán de seguir para asegurar su protección especial. En los artículos citados, se menciona que;

“Artículo 9.- Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca.

No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.

Artículo 10.- No será necesario el consentimiento para el tratamiento de los datos personales cuando:

- i. Esté previsto en una Ley;*
- ii. Los datos figuren en fuentes de acceso público;*
- iii. Los datos personales se sometan a un procedimiento previo de disociación;*
- iv. Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;*
- v. Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;*
- vi. Sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el consentimiento, en los términos que establece la Ley General de Salud y demás disposiciones jurídicas aplicables y que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente, o*
- vii. Se dicte resolución de autoridad competente.”*

El propósito de los artículos citados, es asegurar que el uso de datos sensibles sea ético, y velando por el interés de los usuarios. Por la naturaleza de los datos, se establece que el consentimiento tendría que ser por escrito y con firma del titular. Esto hace sentido, entre más íntimo sea el contenido de un dato, más rígidas deberían de ser las medidas para acceder al mismo. Si el artículo 9 fuera el único que regulara el tratamiento de datos sensibles, Meta, Google, Apple, y todas las demás empresas tecnológicas tendrían que recibir nuestras firmas autógrafas o electrónicas antes de considerar darle tratamiento a nuestros datos. Sin embargo, el problema recae posteriormente en el artículo 10, específicamente en su fracción IV.

³⁵ “Datos personales sensibles: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.”

Este artículo contiene un enlistado de supuestos en los cuales sí se podría acceder a un dato sensible sin conseguir el consentimiento de su titular. Igual que lo establecido en el artículo noveno, los supuestos mencionados suenan totalmente razonables. En casos de emergencias, o cuando una autoridad requiera cierta información, hace sentido que el consentimiento del titular pasara a segundo plano. Sin embargo, la fracción IV, establece que no habrá necesidad de buscar consentimiento del titular cuando se “tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable”. Aquí, es donde entran en juego los términos y condiciones, y también donde cualquier intento de proteger los datos sensibles se tira a la basura.

Para efectos del supuesto anterior, los términos y condiciones fungen como un contrato donde las partes son la plataforma digital, y el usuario. Aquí, el usuario manifiesta su voluntad por vía electrónica para aceptar los lineamientos establecidos por la plataforma para acceder a la misma. Esta operación causa una relación jurídica donde se crean derechos y obligaciones. Es decir, todas las plataformas digitales que tengan términos y condiciones necesarios para acceder a su servicio podrán dar tratamiento a los datos personales sensibles de sus usuarios sin obtener un consentimiento expreso.

El problema aquí, como se expuso en la sección de “Casos Trascendentales”, es que al no ofrecerle al usuario una manera adecuada para “opt-out” o manifestar su voluntad con respecto de sus datos personales sensibles, se incurre en violaciones a su privacidad. Lo dispuesto en el artículo 10 fracción IV de la ley citada prácticamente hace que las violaciones cometidas en el caso de “Google vs. Estado de California” y “Flo vs. FTC” sean en México, prácticas no solamente permitidas, si no, legales. Esto porque la disposición citada implica que siempre y cuando un usuario hubiera aceptado términos y condiciones, entran en una relación jurídica con la plataforma digital, y por ende, no tendrían que dar su consentimiento expreso para compartir datos sensibles como de ubicación, médicos o bancarios.

Bajo una interpretación aislada de la disposición (es decir, sin tomar en cuenta otros artículos de la misma ley), se pudiera asumir que se vuelve nula la necesidad de dar avisos de privacidad a los usuarios de plataformas digitales.

Es incongruente fingir tener disposiciones que protegen a los datos sensibles de los usuarios, cuando quienes más dan tratamiento a los datos sensibles a los usuarios son los mismos que tienen permiso especial de hacerlo.

2. DE LOS DERECHOS ARCO

A parte del derecho a la vida privada, existen los derechos ARCO. Los derechos ARCO se rigen por la LFPDPPP, y refieren a 4 derechos distintos. Estos son los derechos de acceso, rectificación, cancelación y oposición- y son derechos que todos los titulares de los datos personales podrán tener. El ejercicio de estos derechos será gratuito, y accesible. En su artículo 22, la LFPDPPP refiere al ejercicio de los derechos ARCO como:

*“Artículo 22.- Cualquier titular, o en su caso su representante legal, podrá ejercer los derechos de acceso, rectificación, cancelación y oposición previstos en la presente Ley. **El ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio de otro.** Los datos personales deben ser resguardados de tal manera que permitan el ejercicio sin dilación de estos derechos.”*

El artículo anterior sirve para dar a entender que los derechos ARCO pueden o no ser mutuamente exclusivos, es decir, no es necesario el ejercicio de uno para buscar el ejercicio de otro. Estos cuatro derechos se “juntan” en su nombre, porque todos son derechos que nacen del derecho a la protección de datos personales. Estos derechos son como vías para asegurar que los titulares de datos personales estén protegidos ante los responsables que almacenan o dan tratamiento a sus datos. Para dar a entender las funciones de estos derechos, primero se debe entender que cuando se habla de “responsables” en la LFPDPPP se refiere a quien almacena, compra, vende o da tratamiento a datos personales. Partiendo de esta definición, comenzamos a desglosar los derechos mencionados.

El primer derecho, es el derecho al acceso. Mediante el mismo, se busca asegurar que los titulares de datos personales puedan solicitarle al responsable, acceder a sus datos personales o revisar cuales son los datos que cedieron. La obligatoriedad de los avisos de privacidad son en función del derecho al acceso, ya que se obliga al responsable a dar a conocer todos los datos que están en su poder, y esta es la primera forma en la que el usuario puede acceder a información relevante a sus datos personales. También, está el derecho a la rectificación de los datos, donde se busca permitir al usuario de asegurarse de que los datos atribuidos a su persona sean correctos. Este derecho resulta ser muy útil, porque hay muchas veces donde se proporcionan datos equivocados a distintos responsables. El derecho a la cancelación sirve para que el usuario de los datos personales pueda pedir que se cancele algún dato del cual es titular, y que está siendo almacenado o utilizado por el responsable. Una forma en la cual se podría ejercer el derecho a la cancelación, sería utilizándolo para borrar un número telefónico que está en la base de datos de un banco, por ejemplo. A pesar de ello, la modalidad en la cual se lleva a cabo el derecho de la cancelación puede implicar más trabas que los demás derechos ARCO. Se observa en el artículo 25 de la LFPDPPP lo siguiente;

“Artículo 25.- El titular tendrá en todo momento el derecho a cancelar sus datos personales.

La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. El responsable podrá conservarlos exclusivamente para efectos de las responsabilidades nacidas del tratamiento. El periodo de bloqueo será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en los términos de la Ley aplicable en la materia.

Una vez cancelado el dato se dará aviso a su titular.

Cuando los datos personales hubiesen sido transmitidos con anterioridad a la fecha de rectificación o cancelación y sigan siendo tratados por terceros, el responsable deberá hacer de su conocimiento dicha solicitud de rectificación o cancelación, para que proceda a efectuarla también.”

Como se podrá analizar del artículo anterior, la cancelación de un dato no es absoluto, ya que queda sujeta a distintas condiciones como las responsabilidades del tratamiento (las cuáles no son claras ya que no se ejemplifica cuáles pudieran ser dichas responsabilidades) y también, las prescripciones de las acciones derivadas (igual, no se ofrece una aclaración donde se de a entender a qué se refiere con eso). Estas especificaciones son sumamente confusas y vagas, dejando mucho del ejercicio del derecho de cancelación a disposición de la interpretación del responsable. También, parece pertinente tomar en cuenta que se utiliza

la frase “suspensión del dato” en vez de “cancelación del dato”. El lenguaje es importante, y hablar de una suspensión puede dar a entender que se detiene temporalmente el uso del dato, más no se “cancela” en su totalidad.

Otra de las fallas de la regulación del derecho a la cancelación se encuentra en el artículo 26 de la LFPDPPP, donde se establece lo siguiente:

“Artículo 26.- El responsable no estará obligado a cancelar los datos personales cuando:

- I. Se refiera a las partes de un contrato privado, social o administrativo y sean necesarios para su desarrollo y cumplimiento;*
- II. Deban ser tratados por disposición legal;*
- III. Obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas;*
- IV. Sean necesarios para proteger los intereses jurídicamente tutelados del titular;*
- V. Sean necesarios para realizar una acción en función del interés público;*
- VI. Sean necesarios para cumplir con una obligación legalmente adquirida por el titular; y*
- VII. Sean objeto de tratamiento para la prevención o para el diagnóstico médico o la gestión de servicios de salud, siempre que dicho tratamiento se realice por un profesional de la salud sujeto a un deber de secreto.”*

En la primera fracción, se refiere a las obligaciones que derivan de los contratos privados como excepción al derecho de cancelación. Por este lado, no se causa un perjuicio mayor a los usuarios ya que los contratos de adhesión (es decir, los términos y condiciones de las plataformas digitales) por su naturaleza unilateral y sin lugar a la negociación, no son ampliamente considerados como contratos privados.³⁶ Sin embargo, si ponemos atención a la fracción 6 del mismo artículo, veremos que otra de las excepciones son los datos necesarios para cumplir una obligación legalmente adquirida por el titular. Aquí es donde el derecho de cancelación pudiera ser negado a todos aquellos que accedieron a un contrato adhesivo, ya que por más que no sean contratos privados, si son contratos que crean obligaciones legales para los titulares. Bajo este supuesto, ningún titular de datos personales pudiera tener seguridad la cancelación de su información en el caso de haber aceptado los términos y condiciones de alguna plataforma digital. Es decir, el derecho a la cancelación en casos donde se aceptaron términos y condiciones, serían sujetos a la voluntad del responsable. Estas disposiciones dejan sin protección a los usuarios de todo tipo de plataforma digital.

³⁶ Rojina Villegas, Rafael. **Compendio de Derecho Civil**. Vigésima Edición. México, Editorial Porrúa., 1990, p.37

Por último tenemos al derecho a la oposición, el último de los derechos ARCO. Como menciona su nombre, este derecho es el que se ejerce para que el titular pueda oponerse a la captación y el tratamiento de sus datos personales. Parecería que este derecho sería el más desarrollado en cuestiones de su legislación, ya que lo más sencillo sería que los usuarios pudieran oponerse al tratamiento de sus datos antes de que se llevara a cabo para evitar molestias posteriores. Sin embargo, el derecho a la oposición es un tema tocado muy por encima en la legislación. Con respecto del último, solamente se establece lo siguiente en el artículo 27 de la LFPDPPP:

*“Artículo 27.- El titular tendrá derecho en todo momento **y por causa legítima** a oponerse al tratamiento de sus datos. De resultar procedente, el responsable **no podrá tratar los datos relativos al titular.**”*

Considerando que es el único capítulo que refiere exclusivamente al derecho de oposición, deja mucho que desear, ya que no se establecen directrices para determinar qué sería una causa legítima para oponerse al tratamiento de sus datos. Para empezar, considero que no querer que traten tus datos es causa legítima suficiente. Es posible que parte de la razón por la cual no se desarrolla tanto el tema del derecho a la oposición es porque el aviso de privacidad supone tener la finalidad de ser transparente con respecto del tratamiento de datos, para que el usuario tenga la opción de oponerse. Sin embargo, el problema con los avisos de privacidad (como hemos visto en capítulos anteriores) es que solo son transparentes con los datos que ya fueron utilizados, es decir, solo da lugar a la oposición posteriormente a su tratamiento en vez de desde antes de su origen.

3. DEL INAI

A lo largo de este texto, se ha aludido al INAI en distintas ocasiones, pero ¿qué es? Y ¿qué protecciones les ofrece a los titulares de datos personales? El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) es el organismo autónomo constitucional que tiene como finalidad asegurar que los gobernados

puedan acceder a información pública, así como salvaguardar su propia información. El INAI tiene distintas funciones, pero en cuanto a transparencia y acceso a la información, lucha para garantizar la rendición de cuentas mediante accesibilidad a información que pueden buscar los particulares (especialmente información que está en manos de autoridades, esto para salvaguardar el derecho constitucional de petición). También, el INAI funge como autoridad sancionadora para las personas físicas o morales que promuevan prácticas, actos, o legislaciones que vulneran los derechos y datos personales de los gobernados.³⁷

Las funciones del INAI se rigen por la constitución en su artículo 6to fracción A inciso VII. Con respecto de las atribuciones del INAI, se dicta lo siguiente:

“La Federación contará con un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados en los términos que establezca la ley.

El organismo autónomo previsto en esta fracción, se regirá por la ley en materia de transparencia y acceso a la información pública y protección de datos personales en posesión de sujetos obligados, en los términos que establezca la ley general que emita el Congreso de la Unión para establecer las bases, principios generales y procedimientos del ejercicio de este derecho. En su funcionamiento se regirá por los principios de certeza, legalidad, independencia, imparcialidad, eficacia, objetividad, profesionalismo, transparencia y máxima publicidad. El organismo garante tiene competencia para conocer de los asuntos relacionados con el acceso a la información pública y la protección de datos personales de cualquier autoridad, entidad, órgano u organismo que forme parte de alguno de los Poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicatos que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal; con excepción de aquellos asuntos jurisdiccionales que correspondan a la Suprema Corte de Justicia de la Nación, en cuyo caso resolverá un comité integrado por tres ministros. También conocerá de los recursos que interpongan los particulares respecto de las resoluciones de los organismos autónomos especializados de las entidades federativas que determinen la reserva, confidencialidad, inexistencia o negativa de la información, en los términos que establezca la ley....”

Igualmente, la misma Constitución nos remite a la LFDPPP, donde se adentra más con respecto de las facultades que tiene el INAI más allá de la encomienda de proteger los datos personales. En su artículo 39, la LFDPPP incluye un enlistado de las atribuciones del organismo, donde se desglosa de la siguiente manera:

³⁷Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). “¿Qué es el INAI?”. México. Disponible en línea: INAI <https://home.inai.org.mx/?page_id=1626> (Consulta: Septiembre 2024)

“Artículo 39.- El Instituto tiene las siguientes atribuciones:

- I. Vigilar y verificar el cumplimiento de las disposiciones contenidas en esta Ley, en el ámbito de su competencia, con las excepciones previstas por la legislación;*
- II. Interpretar en el ámbito administrativo la presente Ley;*
- III. Proporcionar apoyo técnico a los responsables que lo soliciten, para el cumplimiento de las obligaciones establecidas en la presente Ley;*
- IV. Emitir los criterios y recomendaciones, de conformidad con las disposiciones aplicables de esta Ley, para efectos de su funcionamiento y operación;*
- V. Divulgar estándares y mejores prácticas internacionales en materia de seguridad de la información, en atención a la naturaleza de los datos; las finalidades del tratamiento, y las capacidades técnicas y económicas del responsable;*
- VI. Conocer y resolver los procedimientos de protección de derechos y de verificación señalados en esta Ley e imponer las sanciones según corresponda;*
- VII. Cooperar con otras autoridades de supervisión y organismos nacionales e internacionales, a efecto de coadyuvar en materia de protección de datos;*
- VIII. Rendir al Congreso de la Unión un informe anual de sus actividades;*
- IX. Acudir a foros internacionales en el ámbito de la presente Ley;*
- X. Elaborar estudios de impacto sobre la privacidad previos a la puesta en práctica de una nueva modalidad de tratamiento de datos personales o a la realización de modificaciones sustanciales en tratamientos ya existentes;*
- XI. Desarrollar, fomentar y difundir análisis, estudios e investigaciones en materia de protección de datos personales en Posesión de los Particulares y brindar capacitación a los sujetos obligados, y*
- XII. Las demás que le confieran esta Ley y demás ordenamientos aplicables.”*

Conforme a la cita anterior, reconocemos que el INAI cuenta con muchas atribuciones que se podrán analizar, pero para efectos de desglosar los puntos que resultan en protecciones, se mencionarán los puntos vistos en los incisos III, VII, X y por último, VI.

En primer lugar, con respecto del inciso III, considero que es una atribución trascendente no solamente por sus efectos materiales, si no, por sus efectos simbólicos. ¿A que me refiero con esto? A lo largo de esta tesis hemos visto, que la mayoría de las plataformas digitales le atribuyen la responsabilidad de proteger datos personales a los usuarios. Quien quiera proteger sus datos deberá de ser diligente en leer los avisos de privacidad y los términos y condiciones, a ajustar las configuraciones de sus dispositivos para permitir o no el uso de “cookies” o modos de rastreo y demás. Sin embargo, el INAI a través de esta lista nos asegura tácitamente, que a quien le corresponde proteger los datos personales, es a los responsables, y no a los titulares de los mismos. El hecho de que el INAI busque emitir recomendaciones para los responsables y no los titulares sirve como un

reconocimiento de que los únicos que nos pueden garantizar la protección de datos personales, son quienes los compran, venden, y dan tratamiento.

Los puntos VII y X van de la mano con el III, ya que al trabajar con las autoridades de supervisión, así como elaborando estudios de impacto es que se podrá emitir recomendaciones más atinadas que pudieran ayudar a los responsables a llevar a cabo mejores prácticas con respecto de los datos personales. También me parece importante que quien es responsable de garantizar la protección de datos personales ofrezca protecciones de naturaleza preventiva y no solamente sancionadora. Es por esto que creo que estas atribuciones son significativas, porque si son llevadas a cabo correctamente, pudieran evitar alguna violación antes de que suceda. El único tema es que las recomendaciones son solo eso: recomendaciones. Al no ser vinculatorias o de carácter obligatorio, las recomendaciones emitidas por el INAI, por más atinadas y útiles que sean, pudieran ser totalmente ignoradas por quienes deberían de tomarlas en cuenta.

Por otro lado, tenemos al inciso X, mismo que consiste en lo que pudiera ser la protección más importante que le puede ofrecer el INAI a los particulares. Esto es la resolución de procedimientos de protección y verificación, así como la respectiva imposición de sanciones a las autoridades responsables. Como se menciona en el artículo, los procedimientos de los que es participe el INAI consisten en 3 diferentes. El procedimiento de protección de derechos, el procedimiento de verificación, y el procedimiento de imposición de sanciones.

El procedimiento de protección de derechos inicia a instancia de partes (específicamente, por parte del titular de derechos), cuando estas aleguen que se ha visto vulnerado su derecho a la protección de datos personales. Aquí, los titulares deberán llenar una solicitud donde se da a entender los preceptos de la LFDPPP que se ve vulnerada, y se menciona la responsable por dicha vulneración. En este procedimiento, el INAI le corre traslado a la responsable con respecto de su solicitud, y en turno la misma deberá de proporcionar pruebas y manifestar lo que en su derecho convenga. Asimismo, el INAI funge

como mediador, ya que está facultado para buscar una conciliación entre las partes a lo largo del procedimiento. Sin embargo, en el caso de que se resuelva que el titular sí tenía la razón en su solicitud, la responsable contará con 10 días para hacer valer los derechos del titular, o en su caso, rectificar el error que se llevó a cabo con respecto de los datos personales del titular.

El procedimiento de verificación es distinto, ya que busca asegurar que se haya llevado a cabo la ejecución de la resolución emitida en el procedimiento de protección, ya que estas son vinculatorias y de naturaleza obligatoria. Esta podrá iniciar a instancia de partes o de oficio, y como mencionamos anteriormente, solo proceden en caso de incumplimiento de las mismas resoluciones emitidas por el INAI.

Finalmente, tenemos el procedimiento de imposición de sanciones. Al igual que el procedimiento de verificación, el procedimiento de imposición de sanciones procede en consecuencia de lo visto en un procedimiento de protección de derechos. Aquí es donde el INAI está facultado para llevar a cabo ciertos “castigos” para responsables que incurren en incumplimiento de la LFDPPP, o que violan derechos de los particulares. Contrario a la creencia popular, este mecanismo en realidad sí ha ayudado a particulares a enfrentarse a empresas grandes con respecto de sus derechos. Por ejemplo, en la tesis de jurisprudencia 2a./J. 2/2024 (11a.), se habla del caso reciente donde el INAI llevó a cabo el procedimiento de verificación, así como el procedimiento de sanciones en contra de la institución financiera CIBanco, por no proteger los datos sensibles de sus usuarios. La sentencia dicta lo siguiente:

“INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES. LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE PARTICULARES Y SU REGLAMENTO, ASÍ COMO LA LEY FEDERAL DE PROCEDIMIENTO ADMINISTRATIVO CONSTITUYEN EL MARCO JURÍDICO QUE DEBE OBSERVARSE EN LOS PROCEDIMIENTOS EN TRÁMITE O QUE SE INICIEN A PARTIR DEL 15 DE OCTUBRE DE 2020.

Hechos: El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) a través de la Dirección General de Investigación y Verificación del Sector Privado con motivo de información publicada en redes sociales tuvo conocimiento de que una institución financiera sufrió una intrusión cibernética que puso en riesgo el resguardo de información que contenía datos personales y patrimoniales de sus clientes. Por ello, en uso de sus facultades constitucionales

concluyó que se incumplió el deber de seguridad y, por tanto, ordenó iniciar el procedimiento de imposición de sanciones. Inconforme con la decisión emitida en el procedimiento de verificación, la institución financiera promovió juicio de amparo en el que, entre otros aspectos, alegó la inconstitucionalidad de diversos artículos de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento. El Juez de Distrito sobreseyó en el juicio de amparo al considerar que los actos reclamados al INAI son de carácter intraprocesal que no generan una afectación de carácter sustantiva; decisión que fue controvertida por la parte quejosa vía recurso de revisión.

Criterio jurídico: La Segunda Sala de la Suprema Corte de Justicia de la Nación determina que en virtud de que el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales el 14 de octubre de 2020 publicó en el Diario Oficial de la Federación el "Acuerdo mediante el cual se aprueba la modificación al anexo del Acuerdo ACT-PUB/25/11/2015.06 mediante el cual se aprueban los Lineamientos de los procedimientos de protección de derechos, de investigación y verificación, y de imposición de sanciones" en cuyo artículo tercero transitorio decidió que a partir del 15 de octubre de 2020 suspendía la aplicación de las disposiciones contenidas en esos Lineamientos; por tanto, las disposiciones contenidas en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento, así como en la Ley Federal de Procedimiento Administrativo constituyen el marco jurídico que debe observarse en los procedimientos en trámite o que se inicien a partir del 15 de octubre de 2020.

Justificación: El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales en términos del artículo 6, apartado A, fracción VIII, de la Constitución Política de los Estados Unidos Mexicanos está facultado para substanciar procedimientos de protección de derechos, de verificación e imposición de multas con el objeto, entre otros, de proteger los datos personales en posesión de particulares. Su actividad vinculada con la verificación del cumplimiento de la ley de la materia y su normatividad se puede activar mediante una denuncia (a petición de parte) o bien de oficio. Ahora bien, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, entre otros, en sus artículos 59 y 60 contiene los lineamientos esenciales de una herramienta legal con que cuenta el Instituto con el objeto de atender a su obligación constitucional de protección de datos personales; asimismo, se delegó a su Reglamento la forma, términos y plazos en que se sustanciará el procedimiento administrativo. En consonancia, de una interpretación sistemática de los artículos 5, segundo párrafo y 65, fracción II, de la Ley de la materia; 128, 129, 131 y 132 de su Reglamento y 16, fracción X, 17 y 60 de la Ley Federal de Procedimiento Administrativo, se obtiene que la etapa de investigación se inicia ante la noticia de una presunta infracción al marco jurídico vinculado con la protección de datos personales y se erige como un prerrequisito para que el INAI despliegue una serie de actos concatenados, que incluso pueden ser de molestia, que deben materializarse con el objeto de definir su posible existencia. Ahora, en términos de los ordenamientos aplicados de manera supletoria, el Instituto goza de tres meses para agotar esa etapa y, en caso de ser positivo el resultado, deberá emitir de manera fundada y motivada una resolución que determine la procedencia del inicio del procedimiento de verificación; de no hacerlo en ese término y transcurridos treinta días más, operará la figura de la caducidad de la instancia."³⁸

³⁸ INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES. LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE PARTICULARES Y SU REGLAMENTO, ASÍ COMO LA LEY FEDERAL DE PROCEDIMIENTO ADMINISTRATIVO CONSTITUYEN EL MARCO JURÍDICO QUE DEBE OBSERVARSE EN LOS PROCEDIMIENTOS EN TRÁMITE O QUE SE INICIEN A PARTIR DEL 15 DE OCTUBRE DE 2020. Semanario Judicial de la Federación y su Gaceta, Décima Época, Libro 70. Tesis de Jurisprudencia. Amparo en revisión. Segunda Sala de la SCJN. Número de Registro 2028024. (SJF: Undécima época, III, Septiembre, 2023, p. 2353). Disponible en línea: SCJN < <https://sjf2.scjn.gob.mx/detalle/tesis/2028024>>

A diferencia de las demás protecciones analizadas, considero que el INAI es un organismo con las herramientas adecuadas para proteger los datos personales de los particulares. La jurisprudencia anterior (así como otros casos donde el INAI ha impuesto sanciones en contra de empresas grandes) comprueba su eficiencia en descubrir y señalar violaciones por parte de responsables de datos personales, a través de sus investigaciones, independiente de si llega un particular a emitir una queja. Considero que, con base en lo establecido en esta sección, el INAI cuenta con las facultades y herramientas necesarias para prevenir violaciones de privacidad, sancionarlas, e inclusive crear planes a futuro para poder establecer prácticas empresariales que son beneficiosas para la compra, venta y tratamiento de datos personales.

CAPÍTULO IV

¿QUÉ TIENE QUE CAMBIAR?

A lo largo de esta investigación, hemos atravesado distintas áreas de la protección de datos personales. Primero, se entró en contexto acerca de la compra, venta, y tratamiento de estos, para comprender que esta práctica no solamente es una realidad, sino, una inevitabilidad, necesaria para muchos de los modelos de negocios utilizados hoy en día. Después, se habló acerca de los tipos de datos personales y de su naturaleza, para en turno aprender el por qué detrás de todos los lineamientos que rigen a la compra, venta y tratamiento de datos. Al abordar distinta normativa, también resultó indispensable hablar de casos específicos que han creado precedente que ha influido en legislación relevante en materia de datos personales. Al analizar estos casos, se logró entender que, si bien es inevitable que se compartan ciertos datos personales, la manera en la cual se comparten deberá ser reglada, y con el consentimiento expreso afirmativo de los usuarios. Mediante estos casos, aprendimos que, compartir datos personales no constituye un problema jurídico. El problema radica en el acceso que tienen los usuarios a entender lo que se está llevando a cabo con sus datos que pueden ser sensibles.

Entendiendo lo anterior, pudimos también abordar las protecciones que existen en México y a nivel internacional, para que los usuarios puedan hacer valer sus derechos con respecto de sus datos personales. Este capítulo será dedicado a examinar las áreas de oportunidad que existe en la legislación que rige la venta de datos personales. Aquí, se realizará un análisis donde se toman en cuenta las medidas que se podrán tomar por parte de distintas entidades para proteger los datos personales. Para lograr esta labor, se tomarán en cuenta las medidas que han sido implementadas por empresas tanto tecnológicas como de distintos giros para asegurar la protección de los datos de sus usuarios. De igual manera, se utilizará la información expuesta dentro de los casos que fueron tratados en la presente investigación. Aquí, se analizarán las medidas que han sido impuestas por las autoridades para mejorar las prácticas de las empresas que han cometido violaciones en contra de la privacidad de sus usuarios. Haciendo lo último, se buscarán áreas de oportunidad para

elaborar propuestas que pudieran ser eficientes si fueran implementadas por autoridades reguladoras y/o legisladores. Realizada esta labor, se expondrá la propuesta final que comprenderá una serie de acciones que podrán ser implementadas para velar por el interés de los usuarios y sus derechos y datos personales.

Como hemos visto a lo largo de este trabajo la protección de datos personales va de la mano con el derecho humano a la vida privada. Tan es así, que globalmente existe legislación, órganos autónomos, y organizaciones dedicadas a salvaguardar los datos personales. Asimismo, existen un sinnúmero de resoluciones judiciales que funcionan como invitaciones para mejorar las prácticas que tenemos en México con respecto de la protección de datos personales. En la tesis aislada Tesis: I.10o.A.6 CS (10a.), se dicta lo siguiente;

“PROTECCIÓN DE DATOS PERSONALES. EL DEBER DEL ESTADO DE SALVAGUARDAR EL DERECHO HUMANO RELATIVO DEBE POTENCIALIZARSE ANTE LAS NUEVAS HERRAMIENTAS TECNOLÓGICAS, DEBIDO A LOS RIESGOS QUE ÉSTAS REPRESENTAN POR SUS CARACTERÍSTICAS.

Conforme al proceso legislativo de la adición del segundo párrafo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, publicada el 1 de junio de 2009 en el Diario Oficial de la Federación, en relación con la interpretación del artículo 11, numeral 2, de la Convención Americana sobre Derechos Humanos, efectuada en diversos criterios emitidos por la Corte Interamericana de Derechos Humanos, el deber del Estado frente al derecho de los gobernados a decidir qué aspectos de su vida deben o no ser conocidos o reservados por el resto de los individuos que integran la sociedad, y que conlleva la obligación de dejarlos exentos e inmunes a invasiones agresivas o arbitrarias por parte de terceros o de la autoridad pública, debe potencializarse ante las nuevas herramientas tecnológicas. Lo anterior, por el efecto multiplicador de los medios de comunicación digitales de Internet y las redes sociales, a través de los cuales se facilita la difusión y durabilidad de su contenido, al permanecer de manera indefinida en los medios electrónicos en los que se publican, sin restricción territorial alguna; constituyéndose así en una constante invasión positiva o negativa, según el caso, a los derechos inherentes al ser humano, vinculados con el mencionado, como son la intimidad, el honor, la reputación, la vida privada y, consecuentemente, la dignidad humana.”³⁹

La compra, venta y tratamiento de datos personales es un tema en la boca de muchísimas jurisdicciones desde hace tiempo. El problema no es la falta de regulación con respecto de este tema, sino más bien, la ineficacia de dicha regulación. De igual manera,

³⁹ Semanario Judicial de la Federación y su Gaceta, Décima Época, Libro 70. PROTECCIÓN DE DATOS PERSONALES. EL DEBER DEL ESTADO DE SALVAGUARDAR EL DERECHO HUMANO RELATIVO DEBE POTENCIALIZARSE ANTE LAS NUEVAS HERRAMIENTAS TECNOLÓGICAS, DEBIDO A LOS RIESGOS QUE ÉSTAS REPRESENTAN POR SUS CARACTERÍSTICAS. Septiembre del 2019, Tomo III, Tribunales Colegiados de Circuito, p.2200, Amparo Directo 535/2018, Registro: 2020564

como hemos ido exponiendo, la ineficacia de las normas que rigen los datos personales, son producto del hecho de que dichas normas no están diseñadas tomando en cuenta que su función es salvaguardar un derecho humano. Es por esto, que a continuación se propondrán propuestas que se pudieran introducir a distintas leyes para asegurar que estas tengan la finalidad de velar por el interés de los usuarios y sus derechos, y no por las empresas tecnológicas.

1. CAMBIAR LA POSIBILIDAD DEL “OPT- OUT”.

Tanto en Estados Unidos como en otras jurisdicciones, el surgimiento de la figura del “Opt-Out” ha sido consecuencia de prácticas invasivas por parte de las empresas digitales. El “Opt-Out” nace como consecuencia de un sinnúmero de litigios en contra de empresas tecnológicas, donde las mismas se ven obligadas a permitir a sus usuarios de optar por no compartir datos al acceder a sus plataformas. El problema del “Opt-Out”, es que, aunque muchas veces se ofrece la opción de no compartir datos, la modalidad de esta opción suele a presentar trabas para el usuario. Usualmente consistentes en documentos largos y confusos donde es difícil determinar a qué opción tendrías que presionar para “Opt-Out”, esta medida preventiva se vuelve poco eficiente.

De igual manera, el problema con el “Opt-out” es que esta opción parte de la base de que las empresas tecnológicas siempre tratarán tus datos personales (inclusive los sensibles) a menos de que hagas algo para impedirlo. Propongo que esto no debería de ser la presunción. Creo que más allá de darle al usuario la opción de no compartir sus datos, deberían de darle al usuario la opción de sí compartirlos. Es decir, la presunción ideal sería que las plataformas digitales no podrían captar datos personales, a menos de que el usuario hubiera hecho todo lo posible para asegurar que esto fuera posible. A diferencia de un “pop-up” donde el usuario se ve orillado a leer todo lo que tiene que hacer para evitar el tratamiento de sus datos, propongo que cada plataforma digital tenga un apartado de tratamiento de datos. Al acceder a este apartado, el usuario interesado en que se utilicen sus datos personales para determinado fin, podrá aceptar términos y condiciones correspondientes. Es así, que compartir datos será

una elección consciente por parte del usuario, y no una decisión que se toma simplemente porque la plataforma te da a entender que no existe otra opción, o que elegir dicha opción es muy batalloso.

2. AMPLIACIÓN DE FACULTADES DEL INAI

El INAI, como hemos visto a lo largo de esta investigación, es el organismo encomendado por la Constitución para proteger los datos personales de los particulares. Igualmente, hemos visto que sus facultades son amplias, sus recursos y herramientas para llevar a cabo investigaciones eficientes (mucho del material utilizado como doctrina para esta tesis fue publicado por el INAI), y sobre todo, si cuentan con la infraestructura para investigar y sancionar a empresas grandes que podrán abusar de los datos personales.

Como se expuso en la sección dedicada al INAI, sabemos que tiene la atribución de emitir criterios o recomendaciones a responsables de datos personales, así como al mismo gobierno. Sin embargo, estas recomendaciones no son obligatorias ni vinculantes. Considero que el INAI, al ser experto en materia de protección de datos personales, debería de tener las facultades para emitir recomendaciones de naturaleza obligatoria. Para lograr esto, se debería de observar una reforma al artículo 39 fracción IV de la LFPDPPP para quedar así:

“Artículo 39.- El Instituto tiene las siguientes atribuciones:

- I. Vigilar y verificar el cumplimiento de las disposiciones contenidas en esta Ley, en el ámbito de su competencia, con las excepciones previstas por la legislación;*
- II. Interpretar en el ámbito administrativo la presente Ley;*
- III. Proporcionar apoyo técnico a los responsables que lo soliciten, para el cumplimiento de las obligaciones establecidas en la presente Ley;*
- IV. Emitir los criterios y recomendaciones **de naturaleza obligatoria**, de conformidad con las disposiciones aplicables de esta Ley, para efectos de su funcionamiento y operación;*
- V. Divulgar estándares y mejores prácticas internacionales en materia de seguridad de la información, en atención a la naturaleza de los datos; las finalidades del tratamiento, y las capacidades técnicas y económicas del responsable;*
- VI. Conocer y resolver los procedimientos de protección de derechos y de verificación señalados en esta Ley e imponer las sanciones según corresponda;*
- VII. Cooperar con otras autoridades de supervisión y organismos nacionales e internacionales, a efecto de coadyuvar en materia de protección de datos;*
- VIII. Rendir al Congreso de la Unión un informe anual de sus actividades;*
- IX. Acudir a foros internacionales en el ámbito de la presente Ley;*
- X. Elaborar estudios de impacto sobre la privacidad previos a la puesta en práctica de una nueva modalidad de tratamiento de datos personales o a la realización de modificaciones sustanciales en tratamientos ya existentes;*

- XI. *Desarrollar, fomentar y difundir análisis, estudios e investigaciones en materia de protección de datos personales en Posesión de los Particulares y brindar capacitación a los sujetos obligados, y*
- XII. *Las demás que le confieran esta Ley y demás ordenamientos aplicables.”*

3. REFORMA AL ARTÍCULO 9 DE LA LFPDPPP Y SU RESPECTIVO MANUAL DE OPERACIONES.

Algo que resultó muy importante a lo largo de esta investigación, fue hacer énfasis en los datos sensibles, y como el tratamiento de cualquier dato pudiera crear un dato sensible que no había sido captado con anterioridad. Es por esto que las normas que rigen los datos sensibles son de suma importancia. Es por esto que, propongo que las bases de datos que contengan datos sensibles de los usuarios únicamente se puedan llevar a cabo cuando el giro de la empresa dependa preponderantemente de dicha base de datos. ¿A qué me refiero con esto? Considero que proponer legislación donde los datos sensibles sean prohibidos en su totalidad de ser tratados y almacenados sería absurdo, ya que existen diversas empresas, instituciones, y organizaciones cuyos servicios dependen del conocimiento de los datos sensibles de sus usuarios. Por ejemplo, un Hospital necesariamente necesitaría alguna especie de base de datos que contenga los datos sensibles de índole médico de sus pacientes para poder ofrecerles un servicio. Si no existiera en los hospitales un récord de los diagnósticos médicos de los pacientes, así como su historial y antecedentes, no se lograría cumplir con el giro de la institución, que es ofrecer asistencia médica. Ahora bien; esta disposición ya existe en el artículo 9 de la LFPDPPP; donde se establece lo siguiente:

“Artículo 9.- Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca.

No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.”

La disposición esta perfecta, pero hay varios puntos que se tendrían que considerar para que en práctica fuera válida la disposición. Por ejemplo; ¿ante quién se debería de justificar la creación de una base de datos personales sensibles? ¿quiénes están facultados para determinar si la base de datos tiene finalidades legítimas? ¿cómo se podrá asegurar el cumplimiento de esta disposición? Es un artículo fallido por el hecho de que sus disposiciones deberían de implicar todo un reglamento que asegure el cumplimiento del mismo.

Es por esto, que propongo reformar al artículo anterior, añadiendo una tabla donde se establecen cuáles serían los tipos de instituciones, empresas u organizaciones que pudieran crear bases de datos que contengan datos sensibles, así como establecer los tipos de datos que se estarían captando o tratando. Como se establece anteriormente, esta lista sería basada en el tipo de responsable cuyo giro depende de acceso a ese tipo de datos. Esta lista comprendería lo siguiente:

Empresa/ Institución/ Organización	Tipos de datos sensibles necesarios para su funcionamiento
Hospitales	Registros de diagnósticos médicos, historial del paciente, etc. Información sensible proporcionada por parte de la aseguradora del paciente. Cualquier otro dato sensible que sea pertinente para llevar a cabo los servicios de salud siempre y cuando han sido proporcionados directamente por el paciente.
Instituciones Bancarias	Registros de información financiera del cliente y movimientos bancarios/transferencias/etc.

	Datos de cuentas bancarias e historial crediticio. Cualquier otro dato sensible que sea pertinente para llevar a cabo los servicios bancarios siempre y cuando han sido proporcionados directamente por el cliente.
Aseguradoras	Datos sensibles proporcionados UNICAMENTE por el asegurado, no por terceros. Registro del historial de reclamaciones. Cualquier otro dato sensible que sea pertinente para llevar a cabo los servicios de seguro siempre y cuando han sido proporcionados directamente por el asegurado.
Instituciones Educativas	Registros académicos de conducta, y demás. Registros de datos proporcionados por maestras y maestros o especialistas de psicología dentro de la escuela. Cualquier otro dato sensible que sea pertinente para llevar a cabo los servicios educativos siempre y cuando han sido proporcionados directamente por el estudiante o su tutor.
Departamentos de Recursos Humanos	Registro de la información laboral del empleado que comprenda nóminas, seguros, antecedentes, etc.

	Registro de evaluaciones por parte de supervisores u otro personal. Cualquier otro dato sensible que sea pertinente para llevar a cabo los servicios de recursos humanos siempre y cuando han sido proporcionados directamente por el empleado.
--	---

CONCLUSIONES

Esta investigación tuvo sus inicios formales al iniciar mi octavo semestre de la carrera de derecho, pero nació a raíz de una serie de preguntas que me mantenían intrigada desde que cursé una clase de Propiedad Intelectual. La investigación nació al hablar de un caso en estados unidos donde se le negó un seguro de gastos médicos a un hombre por información acerca de su salud que ni él mismo conocía. Al hablar de este caso surgieron todo tipo de reflexiones; ¿cómo se capta esta información? ¿quién protege a los particulares del uso de estos datos?, ¿en qué tipo de obligaciones jurídicas incurrimos al compartir datos? ¿cuál es el marco legal que rige este tipo de intercambios?

Esta fue una investigación que cambió de rumbo en múltiples ocasiones, al determinar que, en materia de protección de datos personales, hay mucho terreno por recorrer. Pero, en fin se intentó recorrerlo a lo largo de 4 capítulos destinados hacia el análisis de las deficiencias del marco jurídico cuando se trata de los datos personales.

En el primer capítulo, se buscó entrar en contexto con respecto de la compra, venta y tratamiento de datos personales. Esto fue importante, ya que no solamente se abordó un tema que tiende a ser ignorado, sino también sirvió para entender su intersección con el mundo jurídico. Aquí se exponen los derechos que están ligados con la protección de datos personales, para posteriormente comprender las implicaciones legales de cualquier tipo de operación donde se encuentre información personal de por medio.

En el segundo capítulo se habló acerca de dos casos en materia de datos personales que fueron trascendentales, y que marcaron la pauta con respecto de las prácticas que se deberían de observar por parte de los responsables de los datos personales. En primer lugar, son trascendentales porque sacaron a la luz ciertos problemas jurídicos que el quizás el público general no había contemplado al leer los avisos de privacidad de distintas plataformas digitales. Al dar a conocer los riesgos que se encuentran al compartir datos, se comienza a crear conciencia con respecto de los derechos que se ven violentados a través del

perfilamiento, o las bases de datos que contienen datos sensibles. En segundo lugar, las resoluciones emitidas por las cortes donde se implementan sanciones para las empresas responsables de datos nos ayudan a crear propuestas para prevenir el mal manejo de datos personales.

En el tercer capítulo, se tratan las protecciones actuales para los usuarios de plataformas digitales en México. A través de la distinción de los datos sensibles, el fomento de los derechos ARCO, y las atribuciones del INAI, nacen ciertas obligaciones que deberán de ser cumplidas por parte de los responsables. Sirve también para entender que, aunque las protecciones actuales nos proporcionan un buen punto de partida, aún es importante dar seguimiento a dichas medidas, y mejorarlas. Más que nada, este capítulo establece las bases de nuestro siguiente capítulo, que busca crear propuestas tomando en cuenta la legislación actual en materia de privacidad de datos.

Finalmente, el cuarto capítulo se basa en ofrecer soluciones para un problema que ojalá a lo largo de esta investigación se ha logrado establecer como uno que debería de ser sumamente preocupante para todos. Así es como se llegó a desarrollar el tema de la privacidad de datos.

Ahora bien, mi finalidad con esta investigación se podría limitar a dos puntos. El primero es dar a comprender los alcances de un problema desde un punto de vista jurídico. Hablando desde mi experiencia personal, puedo admitir que mientras siempre estuve consciente de las prácticas invasivas de las plataformas digitales, nunca pensé que estas me pudieran llegar a afectar materialmente. Más aún, nunca me cruzó por la mente que la captación de mi información personal era una vulneración a mis derechos humanos, o a los llamados “derechos de la personalidad”. Considero que es importante dar visibilidad a este problema para exigir legislación que pueda velar por los intereses de los usuarios, y sancionar a los responsables que hacen mal uso de datos ajenos. Especialmente ahorita, cuando se encuentra en discusión la permanencia de órganos autónomos (como el INAI), quienes históricamente han sido los únicos en velar por los intereses de los titulares de datos.

En segundo lugar, se intentó analizar todas las opciones que como usuario tenemos en nuestra disposición para proteger nuestros datos. A pesar de que este problema jurídico es uno que apenas comienza a salir a la luz, es un tema que ha agarrado tracción internacionalmente. La comunidad global ha desarrollado medidas preventivas y soluciones jurídicas para asegurar que se protejan los derechos digitales de los usuarios. De igual manera, las resoluciones emitidas por los altos tribunales (tanto en México como en el extranjero) sirvieron para encontrar las áreas de oportunidad en materia legislativa con respecto de este problema.

En algunos aspectos, la legalidad de la compra, venta, y tratamiento de datos personales fue un tema complicado de abordar. Para empezar, la protección de datos personales, a pesar de ser un derecho constitucional que se rige por la propiedad intelectual, también conlleva implicaciones de muchísimas ramas de derecho. Se podría abordar el tema de privacidad de datos desde una óptica de derecho de las obligaciones o de contratos, al adentrar en el consentimiento, y los contratos adhesivos, y demás. También se pudiera hablar de la privacidad de datos desde la perspectiva del cumplimiento legal en las empresas grandes, hablando de las políticas internas y de los marcos regulatorios que se deberán de observar por parte de los responsables. Se pudiera inclusive hablar de como la segmentación de los datos personales pudiera ser utilizado en el derecho penal, como elemento probatorio. Tener que limitar la investigación sin agarrar tangentes que son sumamente interesantes fue uno de los mayores retos al elaborar este trabajo.

Otro reto significativo a la hora de redactar esta tesis, fue la amenaza constante por parte del poder legislativo en contra del INAI. A falta de las herramientas poner un alto a las prácticas violatorias de las grandes empresas, el INAI ha fungido como un instituto dedicado a velar por los intereses de los titulares de datos personales. Considero que ningún organismo autónomo queda exento de la crítica, pero también creo que los comisionados del INAI han hecho un excelente trabajo en materia de protección de datos. El INAI funciona no solamente por quienes forman parte de este, sino porque sus atribuciones y facultades son las necesarias

para lograr prevenir y sancionar prácticas violatorias de privacidad, independiente de quien las esté llevando a cabo. Estas discusiones por parte del poder legislativo afectó mi investigación a la hora de hablar de las protecciones actuales, así como las propuestas para fortalecer al instituto, ya que hasta la fecha sigo sin estar segura de si el INAI seguirá existiendo a la hora de mi disertación.

También, el tema a tratar es uno relativamente novedoso, por lo que fue difícil partir de bases doctrinales jurídicas más limitadas, en comparación con una investigación acerca de un tema civil o mercantil. Por ejemplo, la biblioteca de la facultad no tenía un solo libro que pudiera ayudarme a investigar mi tema. Sin embargo, este limitante acabo siendo algo bueno para efectos de mi investigación también, ya que al existir más material contemporáneo acerca de mi tema, la modalidad de aprendizaje fue más dinámico. A parte de leer sentencias, leyes, y artículos académicos, pude escuchar podcasts, ver documentales e inclusive “Ted Talks” acerca de mi tema.

Otro beneficio de haber elegido este tema, es su practicidad en el día a día. Al comprender más exhaustivamente los datos que estoy compartiendo, también he logrado ver las formas en las que puedo evitar este tipo de operaciones. Al estar consciente de lo que está en riesgo, puedo tomar decisiones pequeñas que pueden ayudar a limitar la forma en que se captan mis datos. También, he aprendido a navegar los avisos de privacidad y los términos y condiciones para estar consciente de la información que permitiré que se utilice. En general, creo que este es un tema de interés público del cual todos deberíamos de saber, abogados o no.

En los semestres anteriores a comenzar esta investigación, había contemplado varios temas de mi interés que pudieran ser dignos de la realización de una tesis. Más que nada, había intentado de elegir problemas sociales que me habían movido el tapete a lo largo de mi carrera, para dentro de ellos encontrar un problema jurídico, y tratarlo. Pensaba que abordar alguna causa que toda la vida fue importante para mí (como la violencia de género o el medio ambiente) pudiera resultar en una excelente tesis. Quizás y esta idea si era correcta, pero creo

que el resultado alternativo (que fue el que terminó sucediendo) acabo siendo mucho más gratificante. Nunca en mi vida me había preocupado por la privacidad de datos, simplemente no era una causa que me conmovía. Pero en el momento en que comencé a aprender acerca de este tema (casi por accidente), nació una pregunta, una que genuinamente me dejó queriendo saber la respuesta. A pesar de que tenía la idea de efectuar una tesis acerca de un tema que ya dominaba (por mero trámite), terminó siendo una oportunidad para conocer un tema nuevo de mi interés, y saciar todas las preguntas que surgieron al conocerlo.

BIBLIOGRAFÍA

A DOCTRINA.

Acxiom. “**Acxiom consumer data products catalog [PDF]**”, p. 29-40. Disponible en línea: Acxiom <<https://ia801900.us.archive.org/14/items/187222488-acxiom-consumer-data-products-catalog/187222488-Acxiom-Consumer-Data-Products-Catalog.pdf>> Estados Unidos, 2023 (Consulta: Febrero 2024)

Allen, Marshall. “**Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates**”. Estados Unidos: Julio 17, 2018. Disponible en línea: Pro Publica <<https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates>> (Consulta: Febrero 2024)

Bianci, Thiago “**Advertising revenue of Google from 2001 to 2023**”. Brazil: Mayo 22, 2024. Disponible en línea: Statista <<https://www.statista.com/statistics/266249/advertising-revenue-of-google/>> (Consulta: Abril 2024)

Brown, Peter “**US companies must comply with GDPR rule for a local representative**”. 11 de Marzo, 2024. Disponible en línea: New York Law Journal. <<https://www.law.com/newyorklawjournal/2024/03/11/us-companies-must-comply-with-gdpr-rule-for-a-local-representative/>> (Consulta: Marzo 2024)

Davara, Isabel. “**Diccionario de Protección de Datos Personales: Conceptos Fundamentales**”. México: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Primera ed. Noviembre del 2019.

Fadler, Martin y Legner, Christine. **“Data ownership revisited: clarifying data accountabilities in times of big data and analytics”**. Reino Unido: 2022. Disponible en línea: Journal of Business Analytics, Taylor & Francis <<https://www.tandfonline.com/doi/full/10.1080/2573234X.2021.1945961#abstract>> (Consulta: Enero, 2024)

Federal Trade Commission. **“Developer of popular women's fertility tracking app settles FTC allegations it misled consumers about their data privacy”**. Estados Unidos: Enero 28, 2021. Disponible en línea: FTC, News & Press <<https://www.ftc.gov/news-events/news/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc-allegations-it-misled-consumers-about>> (Consulta: Marzo 2024)

Harris Insights & Analytics, LLC. **“2022 Cyber Safety Insights Report- Global Results”**. Estados Unidos: Enero 2022. Disponible en línea: Norton Life Lock <<https://www.nortonlifelock.com/us/en/newsroom/press-kits/2022-norton-cyber-safety-insights-report-special-release-online-creeping/>> (Consulta: Febrero 2024)

Hill, Kashmir. **“Automakers Are Sharing Consumers' Driving Behavior With Insurance Companies”**. Estados Unidos, Marzo 11, 2024. Disponible en línea: New York Times<<https://www.nytimes.com/2024/03/11/technology/carmakers-driver-trackinginsurance.html>>

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) **“¿Qué es el INAI?”**. México. Disponible en línea: INAI <https://home.inai.org.mx/?page_id=1626> (Consulta: Septiembre 2024)

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. **“Guía para la elaboración del Aviso de Privacidad”**. Primera Edición. Mayo, 2022. Disponible en línea: INAI <https://home.inai.org.mx/wp-content/uploads/GuiaElaboracion_AvisoPrivacidad_Area_RH.pdf>

Kang, Cecilia. **“Google reaches \$391.5 million settlement over privacy practices”**. Estados Unidos: Noviembre 14, 2022. Disponible en línea: The New York Times, Tech <<https://www.nytimes.com/2022/11/14/technology/google-privacy-settlement.html>> (Consulta: Marzo 2024)

Lawler, Richard y Shakir, Umar. **“Life360 makes millions selling location data, and it’s about to buy Tile”**. Estados Unidos: 9 de Diciembre del 2021. Disponible en línea: The Verge, Tech. <<https://www.theverge.com/2021/12/9/22820381/tile-life360-location-tracking-data-privacy>> (Consulta: Febrero 2024)

Lomas, Natasha. **“Flo gets FTC slap for sharing user data when it promised privacy”**. Estados Unidos: Enero 13, 2021. Disponible en Línea: Tech Crunch <<https://techcrunch.com/2021/01/13/flo-gets-ftc-slap-for-sharing-user-data-when-it-promisedprivacy/#:~:text=No%20financial%20penalty%20is%20being,notice%20of%20a%20privacy%20action.>> (Consulta: Mayo 2024)

Maheshwari, Sapna, y McCabe, David. **“Congress Passed a Bill That Could Ban TikTok. Now Comes the Hard Part”**. Estados Unidos: Abril 23, 2024. Disponible en línea: The New York Times, Tech <<https://www.nytimes.com/2024/04/23/technology/bytedance-tiktok-ban-bill.html?searchResultPosition=2>> (Consulta: Abril 2024)

Nakashima, Ryan. **“Google Tracks your Movements, Like it or Not”**. Estados Unidos: Agosto 13, 2018. Disponible en línea: Associated Press <<https://apnews.com/article/828aefab64d4411bac257a07c1af0ecb>> (Consulta: Marzo 2024)

Petrosyan, Ani. **“Worldwide digital population 2024”**. Estados Unidos: Octubre 10, 2024. Disponible en línea: Statista <<https://www.statista.com/statistics/617136/digitalpopulationworldwide/#:~:text=Worldwi>

de%20digital%20population%202024&text=As%20of%20January%202024%2C%20there, population%2C%20were%20social%20media%20users> (Consulta: Octubre 2024)

Rojina Villegas, Rafael. **Compendio de Derecho Civil**. Vigésima Edición. México, Editorial Porrúa., 1990, p.37

Ramírez Bañuelos, José Francisco. “**Pautas Para la Aplicación del Principio del Interés Superior del Niño en México**”. México, Noviembre 14, 2021. Disponible en línea: IUS Doctrina Volumen 14, <file:///Users/anamoncayo/Downloads/48953-Texto%20del%20art%C3%ADculo-197271-1-10-20211101.pdf> (Consulta: Septiembre 2024)

Von Hoboken, Joris, Rieke, Aaron, Yu, Harlan, y Robinson, David. “**Data Brokers in an Open Society**”. Open Society Foundation, Londres, 2016.

Wolflord, Ben. “**What is GDPR, the EU’s new data protection law?**”. Suiza, 2020. Disponible en línea: GDPR.EU <<https://gdpr.eu/what-is-gdpr/>> (Consulta: Marzo 2024)

Zang, Jiexing. “**Information Privacy, Data Surveillance and Security—How Australian Privacy Law Fully Plays Its Role in the Age of Big Data.**” Journal of Educational Theory and Management Australia, Synergy Publishing, 2019.

B. LEGISLACIÓN.

Constitución Política de los Estados Unidos Mexicanos. (Promulgada Feb. 5, 1917/Agosto 14,2001).

Ley Federal de Protección al Consumidor. (Promulgada Diciembre 24, 1992).

Ley Federal de Protección de Datos Personales en Posesión de los Particulares. (Promulgada Julio 5, 2010).

Reglamento General de Protección de Datos. Unión Europea. (Vigente Mayo 25, 2018 / Mayo 9 2023)

C. JURISPRUDENCIA.

INFORMACIÓN CONFIDENCIAL. LÍMITE AL DERECHO DE ACCESO A LA INFORMACIÓN (LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL Semanario Judicial de la Federación y su Gaceta, Décima Época, Libro V, Febrero de 2012, Tomo 1, Primera Sala, p. 655, Tesis: 1a. VII/2012, Registro: 2000233. Disponible en https://www.scjn.gob.mx/Transparencia/Documents/CriteriosPJF/Tesis_tematica_Datos_Personales.pdf

PROTECCIÓN DE DATOS PERSONALES. EL DEBER DEL ESTADO DE SALVAGUARDAR EL DERECHO HUMANO RELATIVO DEBE POTENCIALIZARSE ANTE LAS NUEVAS HERRAMIENTAS TECNOLÓGICAS, DEBIDO A LOS RIESGOS QUE ÉSTAS REPRESENTAN POR SUS CARACTERÍSTICAS. Semanario Judicial de la Federación y su Gaceta, Décima Época, Libro 70. Septiembre del 2019, Tomo III, Tribunales Colegiados de Circuito, p.2200, Amparo Directo 535/2018, Registro: 2020564 Disponible en: <<https://sjf2.scjn.gob.mx/detalle/tesis/2020564>>

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES. LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE PARTICULARES Y SU REGLAMENTO, ASÍ COMO LA LEY FEDERAL DE PROCEDIMIENTO ADMINISTRATIVO CONSTITUYEN EL MARCO JURÍDICO QUE DEBE OBSERVARSE EN LOS PROCEDIMIENTOS EN TRÁMITE O QUE SE INICIEN A PARTIR DEL 15 DE OCTUBRE DE 2020. Tesis de Jurisprudencia. Amparo en revisión. Segunda Sala de la SCJN. Número de Registro 2028024. (SJF: Undécima época, III, Septiembre, 2023, p. 2353). Disponible en línea: SCJN <<https://sjf2.scjn.gob.mx/detalle/tesis/2028024>>

D. CASE LAW.

Federal Trade Commission. **Flo Health, Inc. complaint (2023).** [PDF]. <https://www.ftc.gov/system/files/documents/cases/flo_health_complaint.pdf> (Consulta: Marzo 2024)

Office of Oversight and Investigations Majority Staff. **A Review of the Data Broker Industry: Collection, Use and Sale of Consumer Data for Marketing Purposes.** 18 de diciembre del 2013. p. 23. Disponible en línea: Committee on Commerce, Science, and Transportation. United States Senate. <<https://www.commerce.senate.gov/services/files/0d2b3642-6221-4888-a631-08f2f255b577>> (Consulta: Marzo 2024)

(Proposed) Final Judgement and Permanent Injunction, **The People of the State of California v. Google, LLC.** Supreme Court of the State of California for the County of Santa Clara, Estados Unidos: Septiembre 2023. Disponible en línea: <<https://oag.ca.gov/system/files/attachments/press-docs/Google%20Proposed%20Order%20FINAL%20%283%29.pdf>> (Consulta: Marzo 2024)

Superior Court of the State of California for the County of Santa Clara. **THE PEOPLE OF THE STATE OF CALIFORNIA VS. GOOGLE, LLC.** Complaint for Injunction, Civil Penalties, and Other Equitable Relief. Case No. 23CV422424. County of Santa Clara: September 14th, 2023. Disponible en línea: <https://oag.ca.gov/system/files/attachments/pressdocs/Filed%20stamped%20Google%20Complaint.pdf>