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

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS

"PROTECCIÓN DE DATOS PERSONALES A TRAVÉS DE HERRAMIENTAS DE PROCESAMIENTO AUTOMATIZADO DE DATOS: DESAFÍOS Y RECOMENDACIONES"

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

Presenta:

Martha Ivonne Castro Rosas

Asesor:

Dr. Federico César Lefranc Weegan

Ciudad de México, diciembre de 2019

CONACYT
Consejo Nacional de Ciencia y Tecnología

INFOTEC
POSGRADOS

AUTORIZACIÓN DE IMPRESIÓN Y NO ADEUDO EN BIBLIOTECA

MAESTRÍA EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Ciudad de México, 24 de noviembre de 2020
INFOTEC-DAIC-GCH-SE-0625/2020.

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

PROTECCIÓN DE DATOS PERSONALES A TRAVÉS DE HERRAMIENTAS DE PROCESAMIENTO AUTOMATIZADO DE DATOS: DESAFÍOS Y RECOMENDACIONES

Desarrollado por la alumna **Martha Ivonne Castro Rosas** y bajo la asesoría del **Dr. Federico César Lefranc Weegan**; cumple con el formato de biblioteca. Por lo cual, se expide la presente autorización para impresión del proyecto terminal al que se ha hecho mención.

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

Vo. Bo.

Mtra. Julieta Alcibar Hermosillo
Coordinadora de Biblioteca

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

C.p.p Servicios Escolares

Agradecimientos

Mamá, gracias por impulsarme a alcanzar mis sueños y por darme todas las herramientas en tus manos para lograrlo.

Papá, gracias por ser la luz que ilumina mi camino.

Agradezco a mis compañeros de la maestría por hacer de este, un viaje memorable y por abrirme las puertas de su amistad.

Agradezco a mis profesores, por compartir conmigo su experiencia y conocimientos. Especialmente, agradezco al Dr. Federico César Lefranc Weegan por asesorarme en la realización de esta investigación.

Tabla de contenido

Introducción.

La constante incorporación de plataformas digitales a distintos aspectos de las actividades humanas supone una mayor recolección de información personal en tiempo real. Los datos recopilados, puede ser el medio para detectar hábitos de consumo, intereses, interacciones personales, emociones, sentimientos, estados de ánimo, intenciones futuras y hasta predicciones de las relaciones que surgirán entre los internautas.

A su vez, el uso de la inteligencia artificial y otras tecnologías de tratamiento automatizado de datos plantea una nueva forma de procesamiento de información, lo que conlleva un aumento de los riesgos y amenazas del tratamiento de los datos. Además, el grado de perfilamiento que se gesta a través de la analítica avanzada puede revelar aspectos de carácter privado que sin el debido cuidado, puede generar una exposición excesiva de la intimidad de las personas.

Lo anterior, amplifica la necesidad de lograr una gobernanza de los datos con la participación de todos los actores involucrados con la finalidad de construir estrategias de acción para la protección de la privacidad y los datos personales en atención a las legislaciones nacionales e internacionales, las políticas públicas, las mejores prácticas en el sector privado y la incorporación de herramientas tecnológicas para la protección de los datos personales.

Cabe señalar que la inteligencia artificial y otras herramientas de tratamiento automatizado de datos son tecnologías disruptivas que plantean una nueva forma de procesamiento de información, con un gran potencial para el desarrollo humano y su uso esboza mejoras para la industria, el comercio, la investigación y en general, tienen aplicación en prácticamente todos los escenarios que involucren datos. No obstante, su uso enfrenta desafíos para garantizar una protección a los datos personales. Lo anterior plantea hallar alternativas para continuar con su empleo, de cara al respeto de la privacidad de las personas.

La presente investigación tiene como objetivo realizar un análisis del tratamiento de los datos a través de los procesos de analítica de la big data con el fin de vislumbrar los retos y desafíos que el uso de dichas herramientas supone para los derechos de privacidad y de protección de datos personales. Esto conlleva una discusión de los límites difusos que existen entre ambos derechos, la influencia de su ejercicio en relación con otros derechos fundamentales y la importancia de su protección en la Sociedad de la Información y la Comunicación.

A través de la investigación se vislumbrarán algunos de los alcances de la economía de los datos en relación con actividades como el comercio de datos personales, la mercadotecnia digital y el uso de distintas plataformas digitales. Además, se presentará un breve análisis de los procesos de analítica de datos con el fin de conocer sus alcances en relación con el tratamiento de los datos y la posible sobre exposición de la privacidad.

Posteriormente, se realizará un estudio de la legislación nacional en relación con los principales instrumentos jurídicos internacionales de la materia para hacer un ejercicio de derecho comparado y vislumbrar el avance de la protección de tales derechos y su relación con otros derechos humanos. A su vez se pondrán de manifiesto las fortalezas y debilidades de los instrumentos jurídicos en virtud de su eficacia normativa y su impacto en la regulación de las herramientas de procesamiento automatizado y el uso de los datos.

Al final, se emitirá una serie de recomendaciones con el fin de coadyuvar al fortalecimiento de medidas en aras de lograr una protección robusta de los derechos de protección de datos personales y de privacidad en correspondencia con un fortalecimiento de la interoperabilidad entre las actividades estatales y la industria privada.

Capítulo 1

Amenazas y riesgos para la privacidad y la protección de datos personales en el proceso de extracción de información de la big data

Capítulo 1. Amenazas y riesgos para la privacidad y la protección de datos personales en el proceso de extracción de información de la big data

1.1 La economía detrás de los datos.

Las tecnologías emergentes, como la Inteligencia artificial, el Internet de las Cosas, el *blockchain*, las *criptomonedas*, las redes sociales, los dispositivos wearables, el *cloud computing* y la geolocalización son algunas de las tendencias más relevantes en estos momentos, y plantean una nueva forma de comprender el procesamiento de las bases de datos de carácter personal a través de una nueva dimensión.

La ONU estima que el tráfico de datos a través del Protocolo de Internet a nivel mundial, aumentó de 100 gigabytes al día en 1992 a más de 45.000 gigabytes por segundo en 2017 a nivel mundial, además prevé que para 2022 el tráfico IP mundial alcance los 150.700 gigabytes por segundo[1]. Lo anterior es un reflejo de la magnitud de la incorporación de las Tecnologías de Información y Comunicación en la vida de las personas pero sobre todo, del crecimiento del flujo de datos a través del Protocolo de Internet en los últimos años.

El Informe sobre la economía digital 2019 de la ONU estima que esto ha provocado que se geste una nueva "cadena de valor de los datos" que incorpora a las empresas que promueven la recopilación, el almacenamiento, el análisis, la elaboración de conocimiento y la modelización de esos datos[2]. El informe reconoce que la creación de valor surge una vez que los datos se transforman en inteligencia digital y se monetizan a través de su utilización comercial.[3]

Entre los modelos de negocio más rentables de cara a la utilización de los datos, se encuentran aquellos que incorporan a las plataformas digitales como eje para dotar a los usuarios de un medio para interactuar en línea. El informe de la

---

[1] Organización de las Naciones Unidas, *Informe sobre la economía digital 2019*, Creación y captura de valor: repercusiones para los países en desarrollo, United Nations Publications, Nueva York, Ginebra, 2019, p. 12, disponible en http://www.onu.org.mx/wp-content/uploads/2019/09/unctad_esp.pdf (última fecha de consulta el 11 de agosto de 2019).
[2] *Idem.*
[3] *Idem*.

ONU distingue entre dos tipos de plataformas digitales, las de transacción, referentes a los mercados de dos o más vías con una infraestructura en línea que facilita los intercambios entre diversas partes y las plataformas digitales de innovación que crean entornos para que los productores de código y contenido desarrollen aplicaciones y programas[4], estos últimos se desenvuelven como intermediarios e infraestructura y se encuentran los sistemas operativos, de estándar de código y de desarrollo de software para crear programas y aplicaciones[5].

Dentro de las plataformas digitales de transacción que participan de la economía digital se encuentran las empresas como Facebook, Amazon, Uber, Alibaba, Airbnb, eBay, que generalmente actúan como intermediarias entre los oferentes de productos o servicios y los demandantes. Las actividades de estas plataformas, se realizan en torno al comercio electrónico, la comunicación, la difusión de contenido creado por otros usuarios, la intervención en la logística de entrega de productos o como intermediario seguro que absorbe el riesgo de transacciones en línea.

Tales plataformas poseen la capacidad de comunicar, entrelazar y contactar a diversas personas a una escala exorbitantes gracias a su infraestructura física y de sistemas informáticos, no obstante, en muchos casos, la principal fortaleza de estas se deriva de la analítica de los datos que fluyen a través de ellas. La analítica de los datos permite extraer información que dé lugar a predecir patrones de comportamiento, gustos, intereses, intenciones y hasta sentimientos como miedo, felicidad o enojo. Lo anterior permite que las plataformas tengan la información suficiente para mejorar su interfaz con el fin de generar mayores usuario, a la vez que la analítica de ellos brinda la oportunidad de generar campañas focalizadas con el fin de ofrecer soluciones o productos a determinados grupos de personas. Esto supone grandes ventajas competitivas frente a los modelos tradicionales.

[4] *Idem.*
[5] *Idem.*

Entre estas ventajas, se encuentra la facilidad con la que una persona puede tener acceso a bienes o servicios a través de plataformas digitales, la mejora en la calidad de los productos o servicios que se presentan ante ellos a través de las modificaciones realizadas gracias al análisis de indicadores en tiempo real, la inmediatez que otorga la interacción a través del internet, la reducción de tiempos de búsqueda de los usuarios, derivado de la segmentación y al conocimiento de sus preferencias, ubicación geográfica, idioma, entre otras.

Derivado de lo anterior, la economía detrás de los datos ha influido en la creación de nuevos campos disciplinarios tanto en el ámbito académico, de investigación, capacitación y de generación de valor. En este último, cabe mencionar que los diferentes agentes económicos han encontrado un nuevo mundo para desarrollarse como empresas generadoras de software y hardware, de venta de servicios digitales, e incluso como plataformas digitales enfocadas al análisis y extracción de información.

Los terceros que a través del manejo de datos personales ofrecen productos que se derivan de la venta directa o del análisis de los datos, son conocidos como corredores de datos o *data brokers*[6]. Si bien existen otros modelos de negocio cuyo funcionamiento estriba en la recolecta y análisis de información, ya sea a través o sin el uso de medios digitales, como las agencias de mercadotecnia, que por medio de encuestas y cruces de información obtienen datos como los intereses de los grupos de interés. Los data brokers han exponenciado las posibilidades que esto supone, gracias al auxilio de disciplinas como la ciencia de datos, las ciencias sociales computacionales, la minería de datos, los corredores de datos, el marketing digital, comercio electrónico y la incorporación de herramientas de rastreo web.

Para Laura Daniela González Guerrero, los data brokers han revolucionado el manejo de las bases de datos a través de la capacidad tecnológica para recolectar, almacenar, cruzar y analizar volúmenes inmensos de datos de todo tipo,

[6] González Guerrero, Laura Daniela, "Control de nuestros datos personales en la era del *big data:* el caso del rastreo web de terceros", *Estudios. Socio-Jurídicos*, Bogotá, volumen 21, 2019, num.1, June 2019, p. 212.

con diferentes formatos y en tiempo real mediante el uso de tecnología de rastreo en la web[7]. Entre las técnicas que lo data brokers emplean, se incluye el uso de *cookies* para recordar lo que los usuarios realizan en la web a través de la descarga de pequeños archivos que almacenan la interacción de los usuarios.[8]

Sin duda, el uso de plataformas digitales y la recolecta de datos, así como su análisis ofrecen grandes beneficios a las empresas que se allegan de ellos con propósitos comerciales y económicos, los usuarios de ellas también se ven beneficiados frente a las modificaciones que surgen a partir del análisis de los datos recolectados. Sin embargo, además de los beneficios que el uso de plataformas digitales aportan a las empresas y a los consumidores a través de la recopilación y análisis masivo de los datos, con tecnologías como cookies o inteligencia artificial, sus consecuencias alcanzan no sólo a aspectos económicos, sino que también tiene implicaciones sociales, políticas, jurídicas e incluso éticas, que pueden alcanzar incluso planos personales o íntimos de un ser humano. Lo anterior se deriva del tipo de datos utilizados y al tratamiento al que estén sujetos, ya sean datos públicos, personales o sensibles y en consideración a las finalidades de su tratamiento.

1.2 Big data.

Históricamente, la humanidad ha encontrado en la escritura un método de almacenamiento de información que ha facilitado la integridad, calidad y certeza de los datos que en su conjunto eran demasiados para recordar a través de las capacidades de memoria del cerebro humano. La escritura ha sido el medio idóneo para la comunicación, almacenamiento y salvaguarda de información a través del tiempo. Actualmente, se transmite grandes volúmenes de datos, a través de dispositivos digitales y la humanidad ha desarrollado otro tipo de escritura, que se rige por medio de códigos y algoritmos interpretados a través de programas informáticos.

[7] *Ibidem*, p. 213.
[8] *Idem.*

Las interacciones través de medios digitales alimentan enormes bases de datos denominadas como *big data* en las que se escribe, almacena, interpreta y utiliza información en tiempo real, lo que además de generar un rastro que es difícil borrar, teje una nueva realidad segundo a segundo con impacto de alcance global.

De forma general, se entiende que la big data es “toda aquella información que no puede ser procesada o analizada utilizando procesos o herramientas tradicionales.”[9] El Diccionario Español Jurídico define a la big data como el “conjunto de técnicas que permiten analizar, procesar y gestionar conjuntos de datos extremadamente grandes que pueden ser analizados informáticamente para revelar patrones, tendencias y asociaciones, especialmente en relación con la conducta humana y las interacciones de los usuarios.”[10] Otra definición es la hecha por la empresa Gartner, Inc, que describe a la big data como "activos de información de gran volumen, alta velocidad y / o gran variedad que exigen formas rentables e innovadoras de procesamiento de información que permitan una mejor comprensión, toma de decisiones y automatización de procesos."[11]

Es precisamente, la posibilidad de revelar patrones de la conducta humana la que coloca al manejo de este gran volumen de información como un nuevo eje de estudio al considerar el tratamiento de datos personales en tecnologías de información y comunicación.

Además del enorme volumen de datos contenida en la big data, algunos autores sugieren que posee otros atributos. Doug Laney señala que entre sus características se hallan las denominadas *Tres V*, descritas como volumen, variedad y velocidad y que además se materializan como las tres dimensiones de los desafíos en la gestión de datos[12]. Podemos entender, a las

[9] Pérez Marqués, María, *Big Data, Técnicas, herramientas y aplicaciones*, México, Editorial Alfaomega Grupo Editor S.A. de C.V., 2015, p. 9.
[10] Real Academia Española, Diccionario Español Jurídico, disponible en *https://dej.rae.es/lema/big-data Real (última fecha de consulta el 25 de septiembre de 2019).*
[11] Gartner, Gartner Glossary, disponible en *https://www.gartner.com/it-glossary/big-data/*, (última fecha de consulta el 7 de septiembre de 2019).
[12] Laney, Doug, Aplication Delivery Strategies, “3D Management: Controlling Data Volume, Velocity, an Variety”, ApplicationDelivery Strategies, META Group Inc., File 949, 2001, disponible en

Tres V de la siguiente manera: el volumen refiere a la enorme cantidad de datos que caracterizan a la big data; la variedad se instituye en la característica de la heterogeneidad del conjunto de datos y la velocidad refiere a la velocidad con la que se generan[13].

Amir Gandomi y Murtaza Haider agregan nuevos elementos a considerar: la veracidad, la variabilidad y el valor. La veracidad, surge contraposición a falta de fiabilidad; la variabilidad o complejidad, de cara a la necesidad de enlazar, limpiar y transformar los datos y el valor en relación con la posibilidad de aumentar el valor de las bases de datos a través del análisis.[14]

Es destacable la relevancia que el análisis de la big data ha alcanzado como motor para la creación de nuevas tecnologías, métodos, aplicaciones de captura de datos, técnicas de visualización y capacidades de agregación de datos. Para Ashley Braganza y Laurence Brooks, la analítica de big data ha renovado el interés por las matemáticas, las estadísticas y el análisis cuantitativo con base en las prácticas establecidas de inteligencia empresarial, minería de datos y análisis, las metodologías de big data[15].

Si bien, en décadas previas, algunas bases de datos contenían el volumen de información suficiente para ser analizado a profundidad, no existía poder de cómputo capaz ni mucho menos, óptimo para organizar, analizar y encontrar patrones en grandes volúmenes y variedades de datos. Se estima que en el 2019 cada minuto se realizan 4.497.420 búsquedas en Google a nivel global, que al mismo tiempo, las aplicaciones de mensajerías envían 18.100.000 mensajes y se

---

http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf (última fecha de consulta el 3 de octubre de 2019).

[13] *Idem.*

[14]Gandomi, Amir y Haider, Murtaza, "Beyond the hype: Big data concepts, methods, andanalytics", *Journal of Business Research*, s.l.i. Volumen 35, 2015, p. 138, disponible en https://www.sciencedirect.com/science/article/pii/S0268401214001066?via%3Dihub#bib0115 (última fecha de consulta el 21 de agosto de 2019).

[15] Braganza, Ashley, *et al*. "Resource management in big data initiatives: Processes and dynamic capabilities", *Journal of Business Research*, s.l.i., Volumen 70, 2017, enero de 2017, p. 329, disponible en *https://reader.elsevier.com/reader/sd/pii/S0148296316304933?token=F96B045156186A1BB50B0C9825BC60F4EC92B4E3B356481D68104138D7B5F61A99A980D0B238AE47DB00CD45D2670D82 última fecha de consulta el 29 de septiembre de 2019).*

descargan 390.030 aplicaciones[16], por lo cual, y aunado a lo anterior, la variedad de información era ínfima en comparación con la gestada en el presente.

Actualmente, se reconoce que los datos afectan la cultura organizacional y la toma de decisiones basada en evidencia[17] lo que ha propiciado que existe toda una industria basada en ello. En la actualidad, los sistemas de gestión de información y almacenamiento de datos se revisten al análisis como parte de las estrategias comerciales, de mercadotecnia, de los planes de desarrollo de productos, de optimización de procesos y en general, de las actividades estratégicas encaminadas a mejorar la competitividad. La innovación y la eficiencia de las organizaciones ha aumentado al incorporar las tecnologías de analítica de big data, lo que a su vez, propicia que a las bases de datos se revistan de un elevado valor económico.

Por lo anterior, el enorme flujo de información que se transmite a través de plataformas digitales y la voracidad con la que algunas empresas tecnológicas lucran a través del manejo de información personal para desentrañar los hábitos de consumo, preferencias, segmentación de usuarios y predicción de comportamientos, genera cada vez más cuestionamientos sobre las políticas de privacidad de las entidades privadas, así como de los mecanismos de salvaguarda de los datos personales.

1.3 El proceso de extracción de información de las bases de datos.

Para comprender la magnitud de la recopilación de datos que sucede a través de medios electrónicos hay que realizar un análisis de la información que las empresas tecnológicas recopilan, y por otra parte, es relevante hacer un breve análisis de la analítica de los datos para dimensionar el potencial que tiene y los riegos que supone para la privacidad.

---

[16] Domo, *Data Never Sleeps 7.0*, disponible en https://www.domo.com/learn/data-never-sleeps-7 (última fecha de consulta el 1 de octubre de 2019).

[17] Erevelles, Sunil, *et al*., “Big data consumer analytics and the transformation of marketing”, *Journal of Business Research*, s.l.i., 2016, num. 69, p. 897, disponible en *https://www.samiagamoura.com/_media/1.-paper-big-data-marketing.pdf* (última fecha de consulta el 13 de septiembre de 2019).

Con el fin de extraer y así usar la información contenida en los grandes volúmenes de datos, es necesario realizar procesos de analítica de datos. Del procesamiento de la big data se obtendrán indicadores determinantes para la toma de decisiones basadas en evidencia, lo que a su vez arrojará ideas significativas y factores diferenciales en el mercado. Amir Gandomi realiza un estudio de las 5 etapas para extracción de información proveniente de la big data, enunciadas por Labrinidis y Jagadish divididas en dos procesos principales: gestión de datos y análisis[18].

La primera etapa es la gestión de datos, implica los procesos de adquirir, almacenar, preparar y recuperar, analizar y adquirir inteligencia a partir de big data.[19] Entre los procesos señalados con apara su análisis. La segunda etapa es la analítica, que comprende las técnicas para anterioridad, debemos resaltar la necesidad de contar con un consentimiento del titular de los datos personales de conocimiento pleno a los alcances de las finalidades que persigue el responsable[20].

La etapa de gestión de datos, concerniente a los procesos de adquisición y almacenamiento de información resulta de suma relevancia para el tratamiento de datos, pues en es aquí donde surge el vínculo entre el titular de los datos y el responsable de su tratamiento. Aparejado al origen del vínculo, las obligaciones del responsable se manifiestan en la obligación de obtener el consentimiento del titular, en las diferentes modalidades que estudiaremos más adelante, con el objetivo de realiza un análisis de datos de conformidad con los fines manifestados en el aviso de privacidad. Cabe señalar que durante todos los procesos de tratamiento de información que contengan datos personales debe observarse los principios de protección de datos contenidos en las legislaciones de la materia y cuyo análisis se presentará más adelante.

El proceso de analítica de datos conlleva técnicas especializadas para el procesamiento y extracción de información en bases de datos. Amir Gandomi

[18]Gandomi, Amir y Haider, Murtaza, *op. cit*., p. 141.
[19] *Idem.*
[20] *Ibidem* p.140.

detalla algunas de ellas, que se presentarán brevemente a manera de mostrar un panorama general que siente las bases para un entendimiento de la extracción de información con las herramientas de relevancia para el análisis de big data. A su vez, se abordarán algunos de los riesgos que conlleva su uso y se pondrá de manifiesto posibles vulnerabilidades y ejes centrales a considerar para fortalecer el respeto a los derechos de privacidad y protección de datos personales.

1.3.1 Analítica de texto.

La analítica de texto, también conocida como minería de texto, comprende las técnicas que extraen información de datos textuales, conlleva procesos de análisis estadístico, lingüística computacional y aprendizaje automático[21]. Su uso permite analizar grandes volúmenes de texto generados por humanos para hallar y procesar información relevante que posteriormente pueda ser usada. Entre los procesos de analítica de texto se encuentran los relativos a extracción de información; resumen de texto; procesamiento de preguntas; sistemas de control de calidad; técnicas de respuestas a preguntas y las técnicas de análisis de sentimientos, también conocida como minería de opinión[22].

La minería de textos abarcan procesos de extracción de información; resumen; análisis, procesamiento y respuesta a preguntas; control de calidad; procesamiento de documentos y de análisis de sentimientos[23]. Entre los fines para los que se emplea destacan, los de encontrar la relación semántica dela información clave y clasificarla desde categorías sencillas como nombres de personas, de medicamentos, de instituciones y fechas, hasta informes detallados con un complejo uso del lenguaje.

Las técnicas de procesamiento de preguntas y respuestas conllevan un análisis del lenguaje natural emitido por personas, para destacar detalles como el tipo de respuesta buscada, para posteriormente, devolver una respuesta evaluada como la mejor, de conformidad con sistema de control de calidad. Las técnicas de

[21] *Idem.*
[22] *Idem.*
[23] *Idem.*

análisis de sentimientos, también conocidas como minería de opinión[24]; analizan texto para interpretar las opiniones de las personas, esto es útil para conocer la percepción frente a productos, servicios, organizaciones, individuos y eventos[25].

Los sistemas de analítica de texto se han implementado en salud, finanzas, marketing y educación, el turismo, la medicina y el transporte, las finanzas y las ciencias políticas y sociales son las principales áreas de aplicación del análisis de sentimientos. La minería de textos se usa para extraer información de artículos científicos y de noticias, anuncios, correos electrónicos, blogs, redes sociales, foros en línea, respuestas a encuestas, documentos corporativos y buscadores web[26].

De las técnicas de análisis de sentimientos se puede obtener información que para clasificar a los documentos en consideración a los sentimientos positivos o negativos o evaluaciones[27] bajo diferentes estándares como las estrellas o las reacciones de estados de ánimo en Facebook.

Como ejemplo de la analítica de texto, podemos observar la analítica que Google utiliza para mantener a su motor de búsqueda "relevante y úti"[28] por medio del análisis de palabras, frases y fragmentos destacados que guardan una relación entre las los términos buscados y los resultados que se muestran. Para este buscador, no basta realizar una comparación textual, sino que además, emplea una extracción de información en los sitios web que se presentarán como resultado y una selección de los "fragmentos destacados"[29] a mostrar para el usuario de su plataforma. El buscador cuenta con una serie de políticas a cumplir para que una página aparezca en dicha selección entre las que destacan la restricción a páginas

[24] *Idem.*
[25] *Idem.*
[26] *Idem.*
[27] *Idem.*
[28] Sullivan, Danny, *How we keep Search relevant and useful*, disponible en *https://www.blog.google/products/search/how-we-keep-google-search-relevant-and-useful/* (última fecha de consulta el 29 de septiembre).
[29] Google, *How Google's featured snippets work*, disponible en *https://support.google.com/websearch/answer/9351707 (última fecha de* consulta el 8 de octubre de 2019).

que puedan mostrar contenido sexualmente explícito, de odio, violento, peligroso, dañino o de falta de consenso sobre temas de interés público.

Este buscador, no sólo realiza una extracción del texto, sino del interés del internauta, basado en su posible intención e información que se agrega a los términos de búsqueda en relación con los posibles entes que representan, ya sea personas, empresas, lugares, hechos, etc. Tales atribuciones se realizan a partir del estudio histórico de las bases de información con las que cuenta y que se acrecientan a cada minuto, además de un enfoque personalizado en el usuario de su plataforma con base a sus registros históricos de interacción y la segmentación en la que el buscador haya determinado que se encuentra.

1.3.2 Analítica de audio.

La analítica de audio está dedicada a la extracción de información de datos de audio. Se conoce como análisis de habla en el caso de que implique lenguaje humano[30], esta última se rige a partir de tecnologías como el reconocimiento de voz, vocabulario usado, fonética, reconocimiento de idioma y en algunos casos, funciona a través de la transcripción de lo dicho en el audio para posteriormente, ser procesado a través de analítica de texto[31]. Algunas de sus aplicaciones se concentran en los centros de atención al cliente, buscadores web, aplicaciones móviles y recientemente los asistentes personales a base de altavoces.

Las tecnologías de asistentes virtuales, altavoces inteligentes y de internet de las cosas o *Internet of Things* [IoT] son algunos de los ejemplos de implementación de la analítica de audio enfocada en el análisis de habla. Las aplicaciones de tales tecnologías son cada vez más variadas y su uso se ha generalizado en la población. La empresa Loup Ventures realizó un estudio comparativo de la inteligencia de los altavoces Alexa, de Amazon Echo; Google Assistant de Google Home; Siri de HomePod; y de Cortana de Invoke, en el que se determinó la eficacia para comprender el lenguaje natural, eficacia de la respuesta,

[30] Gandomi, Amir y Haider, Murtaza, *op. cit*., p. 141.
[31] *Idem.*

comando, calidad de la información brindada y el tiempo de respuesta[32]. El estudio se realizó a través del análisis de sus respuestas a 800 preguntas hechas por los investigadores.

El estudio arrojó que algunos altavoces obtuvieron puntajes cercanos al 80-90% lo cual indica la eficacia respecto al entendimiento del lenguaje humano y su interacción con los recursos digitales a los que pueden allegarse para emitir respuestas[33]. Los avances en etas tecnologías también pone de manifiesto una nueva manera de interactuar con los dispositivos electrónicos en el que cada vez existe una mayor comprensión de los deseo e intenciones de las personas con una menor cantidad de datos y por supuesto, un nuevo medio de recopilación de información y de creación de perfiles en tiempo real y con acceso a internet.

1.3.3 Analítica de video.

Amir Gandomi señala que la analítica de video, involucra una variedad de técnicas para monitorear, analizar y extraer información significativa de las transmisiones de video en tiempo real y en archivos pregrabados[34].

Entre las tecnologías de analítica de video o de imagen podemos notar un crecimiento detonante y una interconexión de sus usos a través de distintos fines. Entre los potenciales usos de la analítica de video se hallan a través de sitios web, en eventos deportivos, de entretenimiento o en puntos de venta para llevar a cabo el reconocimiento de expresiones faciales, lenguaje e incluso temperatura corporal monitoreada en tiempo real[35].

Ejemplo de lo anterior es la plataforma SnapPay[36] que incorpora la tecnología de reconocimiento facial como medio para autenticar la identidad de una persona al

---

[32] Loup Ventures *, Annual Smart Speaker IQ Test*, disponible en *https://loupventures.com/annual-smart-speaker-iq-test/ (última fecha de* consulta el 7 de octubre de 2019*).*
[33] *Idem.*
[34] Gandomi, Amir y Haider, Murtaza, *op. cit*., 141.
[35] *Idem.*
[36] SnapPay, *SnapPay,* disponible en *https://www.snappay.ca/* (última fecha de consulta el 17 de octubre de 2019).

momento de realizar compras en tiendas físicas o a través del comercio digital[37]. Además, cuenta con soluciones de pago con tecnología de código QR y la evita mostrar datos personales en las transacciones como identidad o datos bancarios de las personas[38]. Esta última solución cuenta con 540 millones de usuarios activos en 26 países y más del 50% de los pagos de comercio electrónico chinos están en Alipay[39].

Lo anterior enmarca un alto nivel de interoperabilidad entre plataformas y un avanzado uso de la tecnología de reconocimiento facial a través de la analítica de vídeo. Esto plantea la recolección de datos biométricos vinculados con información bancaria y de identidad de los usuarios de la plataforma. Además del empleo de esta tecnología en el sector privado, algunos gobiernos han incorporado los mecanismos de identificación de personas a través de rasgos biométricos, lo que por una parte implica una mayor certidumbre y celeridad para la generación de trámites ante instancias públicas, pero también puede desembocar en lo que algunos estiman un Gran Hermano[40].

1.3.4 Analítica de redes sociales.

Se refiere al análisis de datos provenientes de canales de redes sociales. El término redes sociales abarca una variedad de plataformas en línea que permiten a los usuarios crear e intercambiar contenido. Su análisis se puede dividir en analítica basada en contenido y en analítica basada en estructura[41].

La analítica basada en contenido se centra en los datos compartidos por los usuarios, como los comentarios y el contenido multimedia, en este caso se puede

---

[37] *SnapPay, Biometrics SnapPay Merchants Can Now Accept Facial Recognition Payments, disponible en https://www.pymnts.com/news/biometrics/2019/snappay-merchants-can-accept-facial-recognition-payments/ (última fecha de consulta el 17 de octubre).*
[38] *Idem.*
[39] *Idem.*
[40] A través de la novela de ficción “Un mundo feliz”, Aldous Huxley plantea la historia de un mundo distópico en el cual, el control estatal se ejerce a través de la hipervigilancia de los ciudadanos, generada en gran medida a partir de un monitoreo exhaustivo en el que se registran desde hábitos y actividades cotidianas, hasta expresiones faciales.
[41] Gandomi, Amir y Haider, Murtaza, *op. cit*., p. 142.

hacer uso de los sistemas de analítica de texto, audio y video mencionados anteriormente. La segunda está enfocada en los atributos estructurales para extraer la información de las relaciones entre personas, organizaciones y productos[42].

Sin duda, una de las conexiones más íntimas con el mundo es la que se gesta a partir de las conexiones con otras personas, por tal motivo, la recopilación de la información que ocurre en las redes sociales es una de las que revela aspectos más profundos de la personalidad de un individuo. Con el análisis de influencia social se pretende cuantificar la fuerza de las conexiones, los patrones de difusión de influencia en una red y predecir comportamientos futuros en un intervalo de tiempo específico.

Esto supone, claro está, una sobre exposición de la intimidad de cada persona frente a la recopilación de información personal como gustos, intereses, hábitos, aspiraciones e intenciones futuras. Entre los riesgos de este tipo de analítica se vislumbra la posibilidad de la recopilación de todos estos datos sin el consentimiento pleno de los usuarios, la manipulación de los usuarios y en algunos casos, escasos mecanismos de protección de los datos, lo que da lugar al acceso por parte de terceros no autorizados.

El Instituto del Internet de la Universidad de Oxford publicó el reporte “The Global Disinformation Order” en el que se encontró que en el año 2019 más de 70 países se han visto envueltos en campañas de manipulación política en redes sociales con la finalidad de moldear las actitudes públicas a nivel nacional[43] o con el objetivo de controlar la información ya sea para desacreditar oponentes, ahogar opiniones disidentes o coartar el ejercicio de los derechos humanos[44].

El estudio halló que la manipulación computacional de los usuarios de redes sociales hizo uso de algoritmos, automatización y big data con una prevalencia

---

[42] *Idem.*
[43] Bradshaw, *Samantha y* Howard, Philip N., *The Global Disinformation Order 2019 Global Inventory of Organised Social Media Manipulation, Oxford Internet Institute, University of Oxford, 2019, p.1, disponible en https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf (última fecha de consulta el 29 de septiembre de 2019).*
[44] *Idem.*

operativa a través de cuentas falsas, *bots*, humanos y *cyborg*s[45]. Al respecto, Samantha Bradshaw considera que gran parte de la regulación "tiende a centrarse en el contenido" o "problemas al borde de los problemas de desinformación" pero para abordar el problema se debe analizar el algoritmo y el modelo de negocio subyacente.[46] A su vez, este estudio pone de manifiesto no sólo las vulnerabilidades de las redes sociales, sino también la facilidad con la que se puede influir en una gran cantidad de personas a través de ellas.

Esto enmarca un problema enorme no sólo para la regulación, además, es una alerta que debe ser trasladada a una responsabilidad para las empresas privadas, en este caso, a las redes sociales. Esto supone la urgencia de mejorar los mecanismos internos de protección de los usuarios mediante la incorporación de tecnologías que blinden aspectos referentes a los datos y privacidad de las personas que usen su plataforma, a la vez que se requiere de mecanismos tendientes a disminuir la manipulación social a través de tecnologías informáticas.

1.3.5 Analítica predictiva.

Comprende una variedad de técnicas que predicen resultados futuros basados en datos históricos y actuales[47]. Dichas técnicas se subdividen en dos grupos de conformidad con la metodología que empleen, en técnicas regresión y técnicas de aprendizaje automático[48]. A diferencia de otros análisis estadísticos, los convencionales se obtienen a partir de una pequeña muestra de la población y en los de analítica predictiva, las muestras emanan de la big data, lo que significa que son masivas y representan la mayoría de, si no la población total.

La analítica predictiva tiene aplicaciones en numerosas disciplinas, en el ámbito social, se emplea para predecir los próximos movimientos de las personas

---

[45] *Ibidem,* p. 11.
[46]Alba, Davey y Satariano, Adam, “At Least 70 Countries Have Had Disinformation Campaigns, Study Finds.”, *The New York Times*, publicado el 26 de septiembre de 2019, Section B, Disponible en *https://www.nytimes.com/2019/09/26/technology/government-disinformation-cyber-troops.html* (última fecha de consulta el 27 de octubre de 2019).
[47]Gandomi, Amir y Haider, Murtaza, *op. cit*., 142.
[48] *Idem.*

en función con sus características, comportamiento y en consideración con la información que se ha gestado a partir del análisis de datos anteriores o que surjan en el momento de llevar a cabo el proceso de analítica.

En el ámbito de la mercadotecnia digital, la analítica predictiva es útil para predecir comportamientos de futuros o posibles clientes en función de los tipos de análisis que hemos tratado anteriormente, por lo cual, éste proceso puede allegarse de información proveniente de datos de publicaciones en redes sociales, del historial de búsquedas en la web, del historial de ubicaciones registrado por dispositivos weareables, de las instrucciones brindadas a un asistente virtual, de la expresión facial identificada al momento de mirar un producto o incluso, en función de los intereses de las personas cercanas al círculo social de una persona y con las cuales haya habido una interacción constante a través de redes sociales.

Otro de los usos de la analítica predictiva se encuentra en el uso de sistemas informáticos que emiten predicciones sobre la posible reincidencia de personas procesadas por cargos penales. Entre esos sistemas se encuentra la herramienta *Correctional Offender Management Profiling for Alternative Sanctions* [Perfil Correccional de Administración de Delincuentes para Sanciones Alternativas] o *COMPAS* de la empresa Northponte[49]. El estudio realizado por ProPublica[50] sobre los resultados emitidos por COMPAS, exhibe que tal sistema opera con sesgos raciales y un trato diferenciado en función del color de piel.

Al comprobar los pronósticos emitidos por COMPAS en un periodo de dos años, los acusados afro descendientes fueron calificados 45% de las ocasiones erróneamente frente al 23% de los acusados blancos. Esto supone casi el doble de probabilidades de ser clasificados erróneamente en función de su color de piel. Además, los resultados del análisis de reincidencia violenta mostraron que los

---

[49] Northpointe, *Practitioners guide to COMPAS core*, 2015, disponible en *https://www.documentcloud.org/documents/2840784-Practitioner-s-Guide-to-COMPAS-Core.html#document/p30/a296482* (última fecha de consulta el 14 de octubre de 2019).

[50] Angwin, Julia, *et al., Machine Bias There's software used across the country to predict future criminals. And it's biased against blacks, ProPublica, disponible en https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (última fecha de consulta el 3 de septiembre de 2019).*

acusados negros tenían un 77% más de probabilidades de recibir puntajes de riesgo más altos que los acusados blancos[51].

Lo anterior evidencia tres problemáticas principales; en un primer término es cuestionable la recolecta y procesamiento de datos personales sensibles, que dadas las circunstancias del entorno, pueden hacer susceptibles a una persona de discriminación. Al respecto, Jennifer Skeem y Christopher T. Lowenkamp, estiman que el uso de instrumentos que evocan tales diferencias raciales para emitir resoluciones como sentencias puede crear un impacto dispar o consecuencias sociales inequitativas incluso aunque el instrumento midiera perfectamente el riesgo.[52]

En segundo lugar, el ejemplo es relevante para resaltar la importancia de seleccionar cuidadosamente qué tipo de información se recopilará y gestionará en un programa informático para evitar cualquier forma de discriminación derivada de ello. Llegado a este punto, podemos destacar que gran parte de los procesos de analítica de los datos son orientados por personas, que tienen en sus manos la capacidad y responsabilidad de desarrollar programas computacionales que respeten la dignidad humana.

En tercer término, este caso pone de manifiesto que si bien, las herramientas de analítica de big data son útiles para la gestión de una gran cantidad de información, su aplicación no está exenta de errores y requiere de una constante valoración humana para ponderar la eficacia de los procesos de tratamiento automatizado de los datos y por supuesto, la calidad y fiabilidad de los resultados emitidos.

---

[51] Larson, Jeff*, et al.*, *How We Analyzed the COMPAS Recidivism Algorithm*, Propublica, disponible en *https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm* (última fecha de consulta el 3 de septiembre de 2019).

[52] Skeem, Jennifer y Lowenkamp, Christopher T, *"Risk, Race, & Recidivism: Predictive Bias and Disparate Impact", Criminology and Public Policy, Forthcoming, University of Chicago Law & Economics Olin Working Paper, s.l.i., Columbia University, 2010, No. 535,* p. 11, *Disponible en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2687339 (última fecha de consulta el 16 de octubre de 2019).*

Considero que con el fin de disminuir el riesgo de discriminación y el sesgo de error de las decisiones basadas en ello, es importante que los procesos de analítica de datos personales se realicen con de herramientas que incluyan protocolos de anonimización y de desagregación de los datos. Esto por una parte, limita las finalidades del tratamiento de los datos a la obtención de información de carácter general, por ejemplo, análisis estadísticos o de mercadotecnia y por otra parte, disminuye la posibilidad de construir patrones de comportamiento sumamente individualizados y de tomar decisiones basadas en ello, lo que a su vez, rompe con prácticas intrusivas en la vida privada de las personas,

La analítica predictiva tiene estrecha relación con distintos sistemas de tratamiento automatizado de datos como la Inteligencia Artificial o *IA*. La IA es una tecnología relativamente nueva, en 1956, un grupo de científicos en Dartmouth College en los Estados Unidos inició un proyecto de investigación con el objetivo de describir la inteligencia humana de forma tan precisa que una máquina fuera capaz de simularla, lo que se consolidó como "Inteligencia artificial", este concepto también fue conocido como "IA genérica[53].

Si bien, el concepto original de Inteligencia Artificial dista de lo que hoy conocemos como tal, el término se ha vuelo relevante para la analítica de datos. En la actualidad, se entiende como sistema de Inteligencia Artificial a un sistema que con base en el análisis de datos o big data, es capaz de realizar predicciones, recomendaciones o decisiones que influyen en entornos reales o virtuales para un conjunto dado de objetivos definidos por el ser humano. [54] La inteligencia artificial y el aprendizaje automático pueden utilizarse para la búsqueda de una solución

[53] SAP, *¿Qué es la inteligencia artificial?*, disponible en *https://www.salesforce.com/mx/blog/2017/6/Que-es-la-inteligencia-artificial.html* (última fecha de consulta el 5 de septiembre de 2019).
[54] *Idem.*

acertada entre todas las opciones posibles según una acción o la resolución de problema[55] para racionalizar la toma de decisiones mediante una lógica formal."[56]

Si bien, hoy por hoy los procesos de Inteligencia Artificial o de procesamiento automatizado con analítica de datos se encuentran inmersos en prácticamente todas las interacciones que se realizan a través de dispositivos electrónicos y su uso es cada vez más común, con potenciales enormes para mejorar casi todos los aspectos en distintas áreas del quehacer humano como la industria, la salud, la agronomía, la economía, la logística y en cualquier otra área que sea susceptible de un análisis automatizado, su uso tiene implicaciones profundas tanto en la fiabilidad como en el respeto a los derechos humanos.

En este sentido, la Organización para la Cooperación y el Desarrollo Económico considera que la tecnología de Inteligencia Artificia "tiene el potencial de mejorar el bienestar de las personas, contribuir a una actividad económica global sostenible positiva, aumentar la innovación y la productividad, y ayudar a responder a los desafíos globales clave. Se implementa en muchos sectores, desde la producción, las finanzas y el transporte hasta la asistencia sanitaria y la seguridad".[57]

A través de este capítulo se ha expuesto un breve análisis de estas tecnologías, de sus características principales y se ha vislumbrado parte del potencial con el que cuentan para optimizar procesos y fomentar una mayor comprensión del mundo y por supuesto, de la calidad de vida de las personas, sin embargo, también se ha hecho una breve exposición sobre las amenazas de su uso frente al respeto de la privacidad y la protección de los datos personales. Si bien, estas tecnologías son perfectibles y dada su naturaleza se encuentran en una

[55] Organización para la Cooperación y el Desarrollo Económicos, *Recommendation of the Council on Artificial Intelligence*, disponible en *https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449* (última fecha de consulta el 11 de septiembre de 2019).
[56] *¿Qué es la inteligencia artificial?*, disponible en *https://definicion.de/inteligencia-artificial/* (última fecha de consulta el 3 de septiembre de 2019).
[57] Organización para la Cooperación y el Desarrollo Económicos, *Recommendation of the Council on Artificial Intelligence, op. cit.*

evolución constante, es menester atender pautas para agilizar la incorporación de una visión más humana.

Capítulo 2

El derecho humano a la privacidad y a la protección de datos personales en relación con las herramientas de procesamiento automatizado de datos

Capítulo 2. El derecho humano a la privacidad y a la protección de datos personales en relación con las herramientas de procesamiento automatizado de datos

Como se ha expuesto en el capítulo anterior, la incorporación de herramientas de analítica de datos en las plataformas digitales, genera enormes beneficios pero también amenazas y riesgos frente a derechos como la privacidad. La ética y el derecho han tratado de encontrar soluciones para estos temas a través de la emisión de leyes, lineamientos y pautas que buscan otorgar una mayor protección para las personas.

En el presente capítulo se abordará aspectos del derecho de protección de datos personales, del derecho a la privacidad, de los derechos ARCO, los principios del tratamiento de datos y la transmisión de datos a terceros, con la finalidad de valorar la eficacia de los instrumentos jurídicos nacionales e internacionales existentes frente al tratamiento automatizado de datos.

Además, se presentará una serie de consideraciones sobre la privacidad para vislumbrar su importancia, los límites difusos que la envuelven, su relación con otros derechos, especialmente con el de protección de datos personales y se dará paso a un breve análisis de los instrumentos legales que contemplan estas prerrogativas.

2.1 La privacidad como derecho humano frente a las tecnologías de procesamiento automatizado de datos.

Si bien, los límites de la privacidad son algo que depende del contexto cultural y social[58] podemos equipararla con el "derecho del individuo a que lo dejen solo"[59] en

[58] Garzón Valdez, Ernesto, “Lo íntimo, lo privado y lo público”, *Cuadernos de transparencia*, 5ª. ed., México, Instituto Federal de Acceso a la Información Pública, 2008, p.18.
[59] *Warren, Samuel D. y* Brandeis*, Louis D., “The Right to Privacy”, Harvard Law Review, s.l.i, Vol. 4, Num. 5. Diciembre de 1890, p. 217 disponible en https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf (última fecha de consulta el 5 de agosto de 2019).*

este sentido, el derecho a la privacidad es el derecho de controlar el acceso a la información de nosotros mismos[60] y jurídicamente es entendido como la prerrogativa que cualquier persona puede imponer para hacer valer su autodeterminación sobre su información personal y su derecho a la protección de la ley contra injerencias arbitrarias en su vida privada, ataques a su honra o a su reputación[61].

En relación con lo anterior, Ernesto Villanueva y Vanessa Díaz, estiman que lo que caracteriza el derecho a tener una vida privada, es el derecho a mantenerse ajeno a las intromisiones ilegítimas o legítimas pero infundadas[62] para estos autores, lo privado o *privacy* tiene sentido de protección al impedir que los terceros se ocupen de la vida privada de los otros[63].

El derecho a la privacidad supone que sólo el individuo puede levantar el velo que protege su intimidad y si alguien más lo hace, puede en un principio, develar la intimidad de su personalidad[64]. Esto conlleva a concebir que su ejercicio se encuentra enmarcado por la decisión personal de cada individuo, lo que presume la existencia de una libre autodeterminación para hacerlo.

Lo anterior esboza una distinción entre lo público y lo privado, o para ser precisos; entre lo íntimo, caracterizado por su total opacidad; lo público, como la transparencia y entre ambos extremos, el ámbito de lo privado, donde impera una transparencia relativa.[65]

Aunado a lo anterior, la privacidad se deriva del ejercicio de una serie de derechos individuales, entre los que encontramos el derecho de propiedad, de conciencia, de expresión, de decisión sobre la familia, sobre la salud, sobre el

[60] Packard, Ashley, *Digital media law*, 2a. ed., Wiley-Blackwell, s.l.i., 2013, p. 257.
[61] Artículo 16 de la Constitución Política de los Estados Unidos Mexicanos.
[62] Villanueva, Ernesto y Díaz, Vanessa, *Derecho de las nuevas tecnologías (en el siglo XX derecho informático)*, México, Oxford University Press, 2015, p 24.
[63] *Idem.*
[64] Garzón Valdez Ernesto, *op. cit*., p. 22.
[65] *Ibidem,* p.6.

trabajo [66] a su vez, se encuentra entrelazado con otros, como el derecho a la protección de datos personales, a la intimidad, al honor y a la propia imagen.

En la interrelación de tales prerrogativas, se gesta una reciprocidad intrínseca que en algunos casos, dificulta la delimitación de cada derecho. Por otra parte, existe una serie de derechos complementarios que no guardan una relación directa en todos los casos pero que en algunas situaciones se desarrollan paralelamente como los derechos de acceso a la información y el de libertad de expresión.

Tal clasificación puede vislumbrarse con límites difusos al incorporar el uso de las plataformas y nuevos dispositivos digitales. Si bien, el derecho a la protección de la privacidad tiene alcances reactivos derivados de su vulneración, debe constituirse principalmente como un derecho de prevención ante posibles intromisiones ajenas a aspectos íntimos o privados de una persona y los riesgos que esto conllevaría.

Como se ha planteado en el capítulo anterior, la manifestación de actitudes, gestos, estados de ánimo y deseos transitorios, hábitos, interacciones sociales e interacciones con la misma plataforma sucede constantemente y son la materia prima para la analítica de datos. Las tecnologías actuales tienen la capacidad de recolectar, analizar y procesar datos a gran escala y de una forma nunca antes vista. Por medio del uso de estas tecnologías, es posible obtener información útil para, conocer profundamente a un gran número de personas lo que deja expuestos aspectos íntimos de la personalidad que en ocasiones dista de la realidad o la aspiración de llegar a ser.[67]

La información obtenida a través de la analítica de datos se ha convertido en una mina de oro, pues gracias a esto, se puede develar información sobre conductas, patrones de comportamiento, intereses de grupos sociales, inquietudes personales y predicciones de comportamiento futuro. Lo anterior permite que a

[66] Escalante Gonzalvo, Fernando, *"El derecho a la privacidad, México", Cuadernos de Transparencia 02,* Instituto Federal de Acceso a la Información Pública, México, 2004, p. 20, disponible en *https://biblio.juridicas.unam.mx/bjv/detalle-libro/1798-cuadernos-de-transparencia-02-el-derecho-a-la-privacidad* (última fecha de consulta el 11 de agosto de 2019).
[67] Garzón Valdez, Ernesto, *op. cit*., p.22.

través de la emisión de los estímulos adecuados se pueda influir de en la psique de las personas, lo que a su vez se transforma en una fuerte influencia en la toma de decisiones como compras, asistencia a eventos, percepción de figuras públicas, momentos históricos o incluso posturas políticas.

El control que las empresas tecnológicas ejercen respecto a lo que se muestra a una persona y lo que se decide ocultar, incide no sólo en la privacidad, sino también en la libre de elección y el acceso a información puesto que, toda intervención en la esfera privada significa una reducción del control individual.[68]

Si bien, la mayoría de esta información es obtenida de forma directa a través del constante intercambio de datos que sucede en tiempo real en las plataformas digitales, algunas bases de datos están compuestas por información de terceros que desconocen que sus datos están siendo procesados con tales tecnologías.

Por lo anterior, es necesario evaluar los retos del modelo de consentimiento informado frente al manejo real de las bases de datos que realiza el responsable, más aun, en consideración con la información que se puede extraer con los procesos de analítica de datos, pues a través de ellos, se puede hallar una nueva gama de datos independientes a los que el titular consintió tratar. Más adelante se abordará más sobre las obligaciones y los derechos derivados de esta relación jurídica.

En México, el derecho a la privacidad se encuentra reconocido como un Derecho Humano en el numeral 6 de la Constitución Política de los Estados Unidos Mexicanos, en el que se contempla la salvaguarda de la esfera privada de las personas de intromisiones arbitrarias y reconoce el control que el titular de los datos tiene el derecho de acceso a sus datos personales o a la rectificación de éstos[69] en los términos y con las excepciones que fijen las leyes.

---

[68] *Idem.*

[69] Fracción III del Artículo 6 Constitucional, adicionada mediante Decreto publicado en el Diario Oficial de la Federación el 20 de julio de 2007.

La Constitución Política de los Estados Unidos Mexicanos reconoce que todas las personas gozarán de los derechos humanos contenidos en dicho instrumento jurídico, así como en los tratados internacionales de los que el Estado Mexicano sea parte[70]. El artículo 133 de tal ordenamiento establece que la Constitución Federal, las leyes del Congreso de la Unión y todos los tratados celebrados y aprobados de conformidad con la legislación, serán la Ley Suprema de toda la Unión. A su vez, la ONU reconoce, que tales prerrogativas recaen en todas las personas sin distinción alguna de nacionalidad, lugar de residencia, sexo, origen nacional o étnico, color, religión, lengua, o cualquier otra condición.[71]

El derecho a la privacidad, aparece en diversos ordenamientos legales de alcance supranacional entre los que se enuncian los siguientes:

El derecho de protección a la vida privada está previsto en el artículo 12 de la Declaración Universal de los derechos humanos de 1948, en el que se estipula que todas las personas tienen derecho a la protección de la ley contra "injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ataques a su honra o a su reputación".

El Artículo V de la Declaración Americana de los Derechos y Deberes del Hombre de 1948 estipula que "Toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar".

El numeral 8 del Convenio para la Protección de los Derechos y las Libertades Fundamentales, reconoce el Derecho al respeto a la vida privada y familiar y lo hace extensivo al respeto del domicilio y de la correspondencia de todas las personas. Además, estipula la no injerencia de la autoridad pública en el ejercicio de este derecho, salvo en casos previstos por la ley y tal medida sea necesaria para la seguridad nacional, seguridad pública, el bienestar económico del país, la

[70] Artículo primero de Constitución Política de los Estados Unidos Mexicanos, Adicionado mediante decreto publicado el 10 de junio de 2011.
[71]Organización de las Naciones Unidas*, ¿Qué son los derechos humanos?,* disponible en *https://www.hchr.org.mx/index.php?option=com_content&view=article&id=448&Itemid=249* (última fecha de consulta el 23 de agosto de 2019).

defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

El artículo 17 del Pacto Internacional de los Derechos Civiles y Políticos de 1966 de igual manera, contempla la protección de la ley contra injerencias arbitrarias o ilegales en la vida privada, su familia, su domicilio o su correspondencia y además, contempla el amparo de la ley contra ataques ilegales a su honra y reputación.[72]

Por su parte, el numeral 11, apartado 2 de la Convención Americana sobre Derechos Humanos, también llamada Pacto de San José de Costa Rica de 1969, ampara al Derecho a la Protección de la Honra y de la Dignidad y establece la protección de la ley contra "injerencias arbitrarias o abusivas en su vida privada, en la de su familia en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación."

Con lo anterior se expone la importancia que el derecho de protección de los aspectos privados de la vida, tiene para la comunidad internacional y su salvaguarda como derecho humano reconocido en diversos instrumentos supranacionales.

2.2 El derecho humano a la protección de los datos personales.

Como se ha presentado anteriormente, los instrumentos internacionales que protegen la vida privada son numerosos, si bien este derecho a influenciado fuertemente a la protección de los datos personales, ambos derechos tienen diferencias que varían desde la precisión del bien jurídico tutelado, que puede converger en algunas ocasiones, hasta el grado de protección de cada uno. A continuación se explorará la protección de los datos personales y su impacto en la esfera jurídica de las personas.

[72] Comisión Presidencial Coordinadora de la política del ejecutivo en materia de Derechos Humanos-COPREDEH, *Pacto Internacional de los Derechos Civiles y Políticos, versión comentada*, Guatemala, 2011, disponible en *http://www.aprodeh.org.pe/documentos/marco-normativo/legal/Pacto-Internacional- de-Derechos-Civiles-y-Politicos.pdf* (última fecha de consulta el 23 de agosto de 2019).

El derecho de protección de datos personales es relativamente novedoso, si bien, su reconocimiento como derecho humano surgió en 1950, en el Convenio Europeo para la Protección de los derechos Humanos y Libertades Fundamentales y en la Convención Americana de los Derechos Humanos de San José, en el que se hace una mención expresa de la protección de los datos confidenciales de las personas, en México, se manifestó de forma expresa hasta el 2002 a través de una ley secundaria.

La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental del 11 de junio de 2002[73], fue un ordenamiento que contempló formalmente los principios básicos en materia de protección de datos en el Capítulo IV a la Protección de Datos Personales en lo correspondiente al sector público y gubernamental. Tal disposición estipuló en la fracción XIV del artículo 3 como sujetos obligados a los pertenecientes al Poder Ejecutivo Federal, al Poder Legislativo Federal, al Poder Judicial de la Federación, a los órganos constitucionales autónomos, a los tribunales administrativos federales y a cualquier otro órgano federal.

Este derecho consolidó su protección a rango constitucional, a partir de la reforma al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, publicada en el Diario Oficial en junio de 2009, en la que México adoptó una postura de salvaguarda a la protección de los datos personales como derecho humano. La reforma constitucional agregó el segundo párrafo del numeral 16 en la que se reconoció la potestad para ejercer los llamados Derechos ARCO, es decir, los derechos al acceso, rectificación, cancelación y oposición al tratamiento de los datos personales en los términos de la ley.

La legislación nacional para la protección de los datos personales en México, está conformada por la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIPG); Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP); la Ley General de Protección de Datos Personales

[73] Ley Abrogada el 9 de mayo de 2016 a través de la publicación en el Diario Oficial de la Federación

en Posesión de los Sujetos Obligados (LGPDPPSO). De esta manera, el Estado mexicano busca proveer a los gobernados de las herramientas necesarias para el reconocimiento y la protección más amplia de sus derechos humanos a través de una interpretación pro persona de las leyes internas y de los tratados internacionales de los que el estado mexicano forme parte para garantizar el libre ejercicio de los derechos mediante la regulación de la autodeterminación informativa.

Para el caso concreto del tratamiento de datos a través de plataformas digitales, la legislación aplicable es la Ley Federal de Protección de Datos Personales en Posesión de Particulares, publicada el 5 de julio de 2010 en el Diario Oficial de la Federación y en vigor a partir del 6 de julio de 2010. El objeto de esta disposición es la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

Por su parte, la Suprema Corte de Justicia de la Nación, estima que "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."[74]

Esto se deriva de la consideración de la protección de los derechos humanos, como la intimidad, el honor, la reputación, la vida privada y la dignidad humana puesto que las herramientas y medios de comunicación digitales facilitan la difusión y durabilidad de su contenido sin restricción territorial[75]. Lo anterior supone una perspectiva actual de la salvaguarda de los derechos humanos a través de las Tecnologías de Información y Comunicación y reconoce expresamente los riesgos de su vulneración por estos medios.

[74] Tesis I.10o. A.6 CS, Semanario Judicial de la Federación y su Gaceta, Décima Época, t. III, Septiembre de 2019, p. 2200.
[75] *Idem.*

A su vez, la tesis I.10o.A.5 CS (10a.) establece que la protección de datos personales constituye un derecho vinculado con la salvaguarda de otros derechos fundamentales inherentes al ser humano,[76] reconocidos en la constitución federal y en los tratados internacionales.

A partir de estas normas, se establece la obligación del Estado para proteger el derecho de las personas a no ser interferidas o molestadas en ningún aspecto de su persona, tanto en ámbitos como la vida privada, el entorno familiar, la forma en que se ve a sí mismo, el cómo se proyecta a los demás, el honor, la intimidad, la dignidad humana, o que permiten el desarrollo integral de su personalidad como ser humano.

De la tesis citada, podemos extraer la estrecha relación que existe entre los datos personales y derechos como el de la privacidad, que hemos abordado anteriormente. Este punto es relevante para el análisis que haremos a continuación, con la intención de no realizar distinciones técnicas entre los derechos presentados, sino que se pretende apreciar como un conjunto de prerrogativas inherentes a los seres humanos con alcances similares.

Si bien es cierto que entre el derecho a la privacidad y el de protección a los datos personales existen diferencias, que se han presentado previamente, también es cierto que entre ambos existe una correlación y para efectos del análisis de su salvaguarda a través de tecnologías de analítica de datos, se abordarán ambos términos con el mismo nivel de relevancia.

2.2.1 Datos personales.

El Derecho a la Protección de Datos Personales, es definido como la protección jurídica respecto a la recopilación, almacenamiento, utilización, transmisión y cualquier otra operación realizada sobre información personal.[77] A su vez, la

[76] I.10o. A.5 CS, Semanario Judicial de la Federación y su Gaceta, Décima Época, t. III, Septiembre de 2019, p. 2199.
[77] Pulido Jiménez, Miguel, *Convergencias y divergencias: Acceso a la Información y la tutela de los datos personales*, *Retos de la protección de dato personales en el sector público*, México, Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, 2011, p.

fracción V del artículo 3, de 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”. La referencia a cualquier información, enmarca una amplia cantidad y subtipos de datos pertenecientes a una persona, lo que como consecuencia, brinda una protección extensa al reconocer el derecho inalienable de su protección.

La definición engloba aspectos amplios tales como el nombre, el teléfono, la dirección personal, la edad, la nacionalidad, lugar de trabajo, color de cabello, datos biométricos y otros, pasando por los datos sensibles como los referentes a la vida familiar, las opiniones políticas, credo religioso, orientación sexual y otras que pudieran colocar en una posición de vulnerabilidad frente a una posible discriminación o ataques personales. Además de los aspectos correspondientes a los datos personales, el derecho a la privacidad y la relación de ambos con otros derechos, también conlleva la protección de la honra y la reputación de las personas contra ataques injustificados de terceros, ya sea por entes privados o públicos.

El gran valor de los datos personales para las instituciones públicas y especialmente para las empresas del sector privado y su reconocimiento como un objeto inmaterial propiedad de los individuos[78], es todo un reto a sortear para garantizar la protección efectiva de los datos personales. Esto se incrementa al introducir el factor tecnológico puesto que el extenso y acelerado uso de tecnologías que permiten el intercambio de datos en tiempo real como la internet, requiere acciones y estrategias sólidas para hacer frente al posible rezago que esto implica para la actualización de políticas públicas, educación digital, consciencia de información personal.

89, disponible en *http://www.infodf.org.mx/comsoc/campana/2012/LIbrozdatosPweb.pdf* (última fecha de consulta el 12 de septiembre de 2019).

[78] Acuña Llamas, Francisco Javier, “La protección de los datos personales y notas sobre los desafíos de internet”, en Recio Gayo, Miguel, (comp.), *La constitución en la sociedad y economía digitales: Temas selectos de derecho digital mexicano*, México, 2016, p. 1.

2.2.2 Datos personales sensibles.

El artículo 3, fracción VI de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares establece una enunciación no limitativa de aquellos datos que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencias sexuales. De lo anterior podemos entrever que los datos sensibles pertenecen a una clasificación especial de los datos personales. Su límite y definición es relevante a la hora de determinar el tratamiento que se le dará para su protección.

Los datos personales sensibles, comprenden una categoría especial, con un tratamiento más estricto para lograr la finalidad de proteger la intimidad del titular de los datos y evitar que su información revele aspectos que pudieran tender a hacerlo susceptible de discriminación o conlleve un riesgo grave para éste. En este sentido, el responsable del tratamiento de los datos deberá realizar esfuerzos razonables para limitar el periodo de tratamiento de los mismos a efecto de que sea el mínimo indispensable.

2.2.3 Datos biométricos.

El tratamiento de los datos biométricos ha alcanzado una mayor relevancia a través de su recopilación, análisis y aprovechamiento en plataformas digitales. Vanessa Díaz considera que los datos biométricos son "todas aquellas características fisiológicas y morfológicas que nos identifican como individuos únicos"[79], el INAI los define como las "propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, atribuibles a una sola persona y que son medibles".[80]

[79] Díaz, Vanessa, "El ejercicio de los Derechos ARCO ante el flujo trasfronterizo de información biométrica" en Téllez Carvajal, Evelyn, (comp.), *Derecho y TIC vertientes actuales*, México, Instituto de Investigaciones Jurídicas de la UNAM, 2016, p. 119.

[80] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, "Guía para el tratamiento de datos biométricos", México, Edición, Marzo 2018, p. 5, Consultada el 27 de julio de 2019, disponible en *http://inicio.ifai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.p*df.

Ambas definiciones concuerdan en que los datos biométricos son características fisiológicas de carácter individual, lo que obedece a diferencias físicas de la anatomía del cuerpo humano. La segunda definición inserta nuevos elementos concernientes a los rasgos de personalidad y de comportamiento atribuibles a una sola persona, bajo la característica de ser medibles. Estos nuevos elementos son destacables al incorporar en su tratamiento a las tecnologías que son capaces de medirlos, de registrarlos, analizarlos, almacenarlos y que a través de procesos de analítica, permiten la toma de decisiones en relación a la información que se puede extraer de ellos.

Por su parte, el Reglamento 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos reconoce en su artículo 4 a los datos biométricos como "los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos."[81]

Los datos biométricos son útiles para distintos procesos, entre los que destacan, los de reconocimiento, de verificación e los de identificación. El reconocimiento que un sistema realiza sobre los datos biométricos implica la aceptación de que los datos se han ingresado previamente, sin embargo, no necesariamente implica verificación o identificación.[82] Por su parte, la verificación es un proceso que se gesta a través de la comparación de datos biométricos nuevos con aquellos que han sido inscritos en el sistema previamente. Esto se realiza para comprobar si la identidad de una persona corresponde con quien dice que es.[83] Por último, en los procesos de identificación se intenta determinar la identidad de una

[81] Reglamento 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
[82] National Science and Technology Council, *Privacy & Biometrics. Building a conceptual foundation.* s.l.i., Createspace Independent Publishing Platform, 2006, p.7.
[83] *Ibidem*, p. 8.

persona. Esto implica recolectar datos biométricos y compararlos con plantillas biométricas existentes[84].

Una plantilla biométrica “es una representación digital de una o más de las características físicas y / o de comportamiento distintas de un individuo”[85]. Es utilizada para realizar comparaciones en los sistemas. Se estima que en las bases de datos biométricos puede inscribirse nuevos conjuntos de datos biométricos o asociarlos ya sea a una persona o a un conjunto existente de datos biométricos recopilados previamente.[86]

No todas las bases de datos que contengan información biométrica corresponden a sistemas informáticos destinados a su procesamiento para algunos de los fines anteriormente expuestos. En algunos casos, son sólo un sistema de almacenamiento para apoyar actividades humanas, como las verificaciones hechas sobre tarjetas o credenciales de identificación.[87]

Si bien, existen distintas finalidades para crea bases de datos y plantillas biométricas, no todas obedecen a procesos de tratamiento automatizado de los datos, no obstante al almacenar datos personales, su tratamiento se rige bajo las legislaciones correspondientes y en atención a los principios, deberes, derechos y prerrogativas que rigen la protección de datos personales

2.2.4 Nueva gama de datos personales.

En el primer capítulo se abordó algunos ejemplos sobre la analítica de datos para extraer información y utilizarla con diversos fines. Esta información tiene múltiples posibilidades para el surgimiento de información útil y procesada que puede ser aprovechada de una manera completamente diferente que como datos aislados.

La nueva generación de software y sistemas especializados para la analítica de la big data, que se suma a este tipo de tecnología puede allegarse incluso de la

[84] *Ibidem*, p. 12.
[85] *Ibidem*, p. 6.
[86] *Ibidem*, p. 5.
[87] *Ibidem, p.12.*

información recopilada por las aplicaciones conectadas en tiempo real que mediante su exploración y análisis puede emitir una nueva serie de información sobre rutinas, patrones de comportamiento, gustos, intereses, miedos, tendencias políticas, orientación sexual o incluso pueden ofrecer información sobre planes futuros o intenciones, lo que a su vez da origen a los perfiles y segmentación de personas con base a sus hábitos digitales.

El historial de búsquedas web a través de un navegador, las pulsaciones del corazón mientras se realiza ejercicio físico, las veces alguien accede al perfil de un amigo en una red social, el tiempo que una persona mira una fotografía, las veces que se escucha una canción e incluso las horas y el tiempo en que se hace uso de los dispositivos digitales reflejan aspectos sumamente íntimos de la personalidad y no sólo revelan datos personales o sensibles, sino que incluso hacen gala de rasgos únicos e individuales de cada persona entre los que destacan gustos, miedos, deseos, emociones y anhelos.

En efecto, la información obtenida a través de la analítica de datos cumple con las características que la ley atribuye a los datos personales, dado que son concernientes personas físicas identificadas o identificables. A su vez, podemos encontrar entre ellos, datos personales sensibles pues que revelan aspectos que pueden acarrear discriminación e incluso evidencian rasgos de personalidad y de comportamiento que pueden ser medibles.

A partir de la analítica de datos con procesos informáticos se puede obtener nueva información que sin las herramientas tecnológicas sería imposible descubrir. A su vez esta información corresponde a los datos de personas físicas identificables, lo que nos sitúa ante una nueva gama de datos que surgen de la recopilación y análisis de datos que se gesta en las plataformas digitales.

Una característica de los datos personales derivados de la analítica es que sin las herramientas informáticas especializadas para el procesamiento de información, no podrían haberse hallado. Es precisamente el uso de herramientas tecnológicas y la comparación entre datos similares lo que deriva en la obtención

de patrones y nueva información investida de una mayor profundidad que los datos no procesados, lo que a su vez da lugar a una mayor exposición y posibilidades de vulneración de la intimidad de los titulares de los datos.

Cabe mencionar que no todos los datos personales que se encuentren digitalizados o hayan pasado por un proceso de analítica forman parte de esta nueva gama de datos personales, sino sólo aquellos que de no haberse sujetado a este procesamiento, no existirían.

La posibilidad de encontrarnos frente a esta nueva gama de datos implica fortalecer la salvaguarda de la intimidad y de los derechos de privacidad y los demás inherentes al mismo, a través de mecanismos que puedan contrarrestar las amenazas y los riesgos de su uso y exposición. Esto supone incorporar nuevas estrategias y tecnologías informáticas para lograrlo, algunos ejemplos son la encriptación de los datos, la desindexación y la privacidad por diseño.

2.3 El habeas data en la big data.

Francisco Javier Acuña Llamas considera que el habeas data es el medio para combatir las decisiones de los responsables de las bases de datos adoptan en torno a los derechos de ARCO[88], también señala que en México aún no se ha detonado la concientización de las personas para controlar su información y decidir quién puede proporcionarla y qué se hace con ella[89]. En lo que de acuerdo a él, se ha denominado como “ausencia de una cultura de la protección de los datos personales” frente a los desafíos de la era digital[90].

El habeas data plantea la protección de aspectos personales de la vida que tienen una relación intrínseca con la esfera personal. Para Carolina Velandia, el derecho de Habeas Data puede describirse en tres facetas, la sustancial, derivada del derecho a la intimidad y el buen nombre; la segunda, correspondiente a un nivel procesal, como mecanismo de protección de otros derechos como el de la dignidad,

[88] Acuña Llamas, Francisco Javier, *op. cit.,* p. 3.
[89] *Idem.*
[90] *Ibidem* p. 5.

la libertad y la igualdad en referencia a la salvaguarda de la autodeterminación informativa y por último, el habeas data como derecho fundamental[91].

La primera faceta es equiparable a lo que en México representa el derecho de privacidad consagrado en el numeral 6 y 16 de la Constitución Federal que reconoce la protección a la privacidad y a los datos personales. La segunda faceta es representada por el proceso previsto en la LFPDPPP para que el titular ejerza sus derechos ARCO y la tercera faceta se manifiesta como derecho fundamental por medio de la protección que alcanza de su reconocimiento en un nivel constitucional y en el plano internacional por medio de los instrumentos internacionales para su protección como derecho humano.

El habeas data en un nivel procesal está presente por medio del mecanismo y andamiaje jurídico que existe para la protección de estos derechos y de forma concreta, para la salvaguarda del ejercicio los derechos de Acceso Rectificación Cancelación y Oposición del tratamiento de los datos personales. De esta forma, el Estado establece que nadie puede interferir con las decisiones individuales porque ninguna puede imponerse por la fuerza.[92] Por ende, tal recurso, permite una vía de control a la esfera de reserva[93] y con ello, el titular de los datos puede decidir qué información o aspectos de su vida pueden ser conocidos y cuáles permanecer reservados.

A su vez, el habeas data establece el derecho de exigir ante las autoridades y los particulares el respeto a estas decisiones de autodeterminación de su información personal en el marco de las leyes aplicables. En este sentido, el habeas data es también un recurso que protege otros derechos derivados del ejercicio de la protección de los datos personales y del derecho a la privacidad, entre

[91] Velandia, Carolina y Prada, Fredy Alexander, “La protección de los datos digitales. Una lectura de la tensión del habeas data en el contexto del cambio de las relaciones sociales que supone internet” en Téllez Carvajal, Evelyn, (comp.), *Derecho y TIC. Vertientes actuales*, México, Instituto de Investigaciones Jurídicas de la UNAM, 2016, p. 188.
[92] Escalante Gonzalvo, Fernando, *op. cit.,* p. 20.
[93] Villanueva, Ernesto y Díaz, Vanessa, *op. cit*., p. 25.

los que se encuentran la protección a la propia imagen, al buen nombre e incluso a la dignidad humana.

Vanessa Díaz y Ernesto Villanueva estiman que “el habeas data no es un cuestión de hermetismo o secreto, sino de otorgar un recurso a la privacidad”[94]. En este tenor, tal recurso es oponible sólo para la protección de aspectos privados que no contravengan disposiciones en contrario o una obligatoriedad de conservar o dar publicidad a los datos. Ambos señalan que el Estado debe garantizar los límites del habeas data en atención a las finalidades de organización, de conocimiento, de seguridad y certidumbre para la toma de decisiones[95]. Entre estos casos, encontramos por ejemplo, los registros de antecedentes penales, de deudores, patrimoniales, económicos, y demás datos que guardan una relación con las obligaciones del titular con el estado o con particulares, en aras de la salvaguarda de los intereses de la comunidad o información que es necesaria para la vida social.

2.4 La autodeterminación informativa.

La autodeterminación informativa es un derecho emanado de la protección a la privacidad de las personas y se manifiesta en la facultad de ejercer el control sobre su información personal. Vanessa Díaz y Ernesto Villanueva, estiman que el habeas data es el género y la determinación informativa es la especie[96], por medio de la cual, el titular de los datos tiene la potestad para decidir sobre la autorización de la circulación de sus datos, así como su potestad para acceder a las informaciones que sobre él se tenga[97]. Lo anterior presupone un derecho de autotutela respecto a la información personal para decidir el tratamiento que se le dará.

Dicho derecho cobra una mayor relevancia al incorporar a las Tecnologías de Información y Comunicación en la ecuación, lo que da como resultado, una nueva manera de entender el tratamiento de datos y de ejercer la autodeterminación

---

[94] *Idem.*
[95] *Ibidem*, p. 35.
[96] *Ibidem,* p. 25.
[97] *Idem.*

informativa para sortear los retos aparejados a la transformación digital. Entre estos se encuentran los avances en telecomunicaciones, la sistematización y la analítica de los datos.

Las nuevas tecnologías derivadas del avance en las telecomunicaciones se manifiestan cada vez más como herramientas disruptivas que se ejecutan como una extensión de lo que sucede en el mundo físico, que en algunos casos tienen alcances mayores, tal es el caso del cruce trasfronterizo de datos, los conflictos derivados de la extraterritorialidad de los hechos y la aplicación de la norma jurídica. De igual forma, cada vez se suman más participantes a la llamada economía de los datos, como los proveedores de hardware y software, en la que se hallan los data brokers, los servicios de almacenamiento de datos en la nube, los sistemas de gestión de información y almacenamiento de datos, la nube como servicio, etc.

2.5 Derechos ARCO.

La Constitución Federal reconoce en el numeral 16 que toda persona tiene el derecho a la protección de sus datos personales al acceso, rectificación, cancelación y oposición del uso de sus datos en los términos que fije la ley, se conoce como Derechos ARCO a tales potestades.

La autodeterminación informativa, plantea que el ejercicio de los derechos ARCO también sean oponibles al tratamiento a través de las plataformas digitales. Esto tiene alcances en aspectos como el almacenamiento de datos en ficheros informáticos, el tratamiento a través de procesos de analítica, la transmisión de datos a terceros e incluso, la elaboración de perfiles con base a los datos personales. Esto conlleva la potestad de otorgar o retirar el consentimiento del titular de los datos para su tratamiento en consideración con las finalidades que los responsables persigan o para la transmisión de su información personal a terceros.

Los derechos ARCO abarcan el derecho de restringir el tratamiento, lo cual supone decidir qué datos pueden ser tratados bajo los fines expuestos en el aviso de privacidad o limitarlo sólo para efectos de las responsabilidades nacidas de la relación jurídica entre el titular y el responsable de conformidad con el numeral 25

de la LFPDPPP y las demás disposiciones legales. Estos derechos tienen alcances incluso frente a los terceros a los que el responsable haya transmitido datos con anterioridad, por lo que éste, tendrá que hacer de su conocimiento la solicitud del titular para que se dé cumplimiento en lo respectivo.

El acceso y la rectificación de los datos suponen un cumplimiento relativamente sencillo por parte de los responsables pues implica brindar información oportuna al titular en los plazos legales, los derechos de cancelación y oposición presentan una complejidad técnica mayor en cuanto a lo respectivo al almacenamiento de información en dispositivos digitales.

Por una parte, el mismo ordenamiento señala que el derecho de oposición se manifiesta como la restricción del tratamiento de los datos sólo a las finalidades que el titular haya dado su consentimiento, a las propias de la relación jurídica que se gesta entre ambos y a las legales. El derecho a la cancelación de los datos plantea que la información personal del titular de los datos debe ser eliminada cuando este así lo solicite, no obstante, este derecho queda sujeto a un periodo de conservación de los datos, que de conformidad al numeral 37 del Reglamento de la LFPDPPP, los plazos de conservación corresponderán a aquellos que sean necesarios para el cumplimiento de las finalidades del tratamiento y en atención a las disposiciones aplicables a la materia de que se trate. Posteriormente, se procederá a un periodo de bloqueo y su posterior supresión. Si bien, la legislación contempla la obligación del responsable a establecer y documentar procedimientos para tales casos, no es clara respecto a los mecanismos de verificación de su cumplimiento.

En México, los derechos ARCO se encuentran regulados en el capítulo III de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. El artículo 28 de la misma ley contempla que el titular o su representante legal podrán solicitar al responsable del tratamiento de los datos en cualquier momento el acceso, rectificación, cancelación u oposición, respecto de los datos personales que le conciernen, para ello, la ley prevé un procedimiento que se tramitará ante el Instituto Federal de Acceso a la Información y Protección de Datos.

A grandes rasgos, el procedimiento consta de una solicitud, en la que debe obrar el nombre del titular y domicilio u otro medio para comunicarle la respuesta a su solicitud; los documentos que acrediten la identidad o en su caso, la representación legal del titular; la descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados, y cualquier otro elemento o documento que facilite la localización de los datos personales.

La solicitud se presentará al responsable de los datos, quien comunicará al titular, en un plazo máximo de veinte días, contados desde la fecha en que se recibió la solicitud de acceso, rectificación, cancelación u oposición, la determinación adoptada, a efecto de que, si resulta procedente, se haga efectiva la misma dentro de los quince días siguientes a la fecha en que se comunica la respuesta.

El procedimiento se iniciará a instancia del titular de los datos o de su representante legal, expresando con claridad el contenido de su reclamación y de los preceptos de esta Ley que se consideran vulnerados. La solicitud de protección de datos deberá presentarse ante el Instituto dentro de los quince días siguientes a la fecha en que se comunique la respuesta al titular por parte del responsable.

La ley otorga el carácter de Responsable a la persona física o moral de carácter privado que decide sobre el tratamiento de los datos personales. Entre las obligaciones del responsable, se encuentran las de informar a los titulares de los datos que se recaba de ellos y con qué fines a través del aviso de privacidad; limitarse al cumplimiento de las finalidades previstas en el aviso; en el caso de que se pretenda tratar los datos para un fin distinto que no resulte compatible o análogo a los fines establecidos en aviso de privacidad, se tiene que obtener nuevamente el consentimiento del titular si el responsable y tomar las medidas suficientes para garantizar que el aviso de privacidad, sea respetado por él o por terceros con los que guarde alguna relación jurídica. Se reconoce con carácter de Tercero a la persona física o moral, nacional o extranjera, distinta del titular o del responsable de los datos.

En un ejercicio de derecho comparado podemos observar a la ley 25.326 de Protección de Datos Personales de Argentina[98] plantea las prerrogativas que podemos equiparar con los derechos ARCO y de forma expresa en su artículo 16, se contemplan a las bases de datos.

Por su parte, el artículo 19 del Reglamento General de Protección de Datos, de la Unión Europea regula al derecho de supresión de los datos de forma equivalente con el llamado derecho al olvido. Para su cumplimiento, la disposición vislumbra el uso de la tecnología disponible. Además, en el caso de que dichos datos se hayan hecho públicos, el o los responsables del tratamiento harán del conocimiento a las instituciones y organismos distintos de la Unión, que el titular ha solicitado la supresión de cualquier enlace a esos datos personales o de cualquier copia o réplica de estos.

El RGPD contempla el derecho de supresión, también conocido como derecho al olvido. A diferencia del contemplado en la legislación nacional, el artículo 17 del RGPD establece de forma expresa la obligación de suprimir los datos teniendo en cuenta la tecnología disponible.

Al respecto, Vanessa Díaz y Ernesto Villanueva señalan que el derecho al olvido forma parte del hábeas data y que la cancelación, supresión o eliminación de esa información en internet puede colisionar frente al derecho de informar, la libertad de expresión y la capacidad de almacenaje de los motores de búsqueda, pues la velocidad de búsqueda de éstos últimos puede significar el fin del olvido.[99]

Como antecedente al derecho de olvido tenemos la resolución del 13 de mayo de 2014 que el Tribunal de Justicia de la Unión Europea emitió tras la consulta prejudicial de la Audiencia Nacional Española interpuso para establecer los alcances interpretativos de la Directiva 95/46/CE[100]. En la resolución se contempla

[98] Ley 25.326 de Protección de Datos Personales de Argentina.
[99] Villanueva, Ernesto y Díaz, Vanessa, *op. cit*., p. 37.
[100] Tal disposición había sido modificada en enero de 2014 tras la propuesta de la Comisión Europea en referencia los hechos penosos o que pudieran afectar el prestigio de una persona o institución. Posteriormente, la Directiva fue derogada por el Reglamento 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

que en determinadas ocasiones, los buscadores están obligados a atender las solicitudes de particulares para eliminar los enlaces a informaciones que les perjudican.

2.6 Principios del tratamiento de datos personales en el procesamiento automatizado de datos.

Los principios y los deberes en materia de protección de datos personales son obligaciones que los responsables del tratamiento deben observar y se encuentran reconocidos en ordenamientos nacionales e internacionales. Los numerales 6 de la LFPDPPP y el artículo 9 de su Reglamento, enuncian la obligación de observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.

El IFAI o Instituto Federal de Acceso a la Información, considera que los principios de protección de datos son "una serie de reglas mínimas que deben observar las personas físicas o morales que tratan datos personales, para garantizar el uso adecuado de la información personal".[101] Por su parte, Lina Ornelas señala que tales principios alcanzan pleno significado desde el reconocimiento de que quien trata datos personales trata datos ajenos y por ello debe utilizarlos con respeto a los derechos del interesado, lo cual enmarca al respeto de la dignidad de la persona, como base fundamental del derecho de protección de datos personales[102].

Lo anterior enuncia la relevancia de observar los principios de protección de los datos desde una perspectiva orientada al respeto de la dignidad del titular de los datos personales y en consecuencia, sobreponer ese respeto a los intereses del responsable durante cada fase del tratamiento.

---

[101] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *¿Cómo ejercer el derecho a la protección de datos personales?,* disponible en *http://inicio.ifai.org.mx/SitePages/Como-ejercer-tu-derecho-a-proteccion-de-datos.aspx?a=m1* (última fecha de consulta el 25 de julio de 2019).

[102] Ornelas Nuñez, Lina y Piñar Mañas, "Los principios de la protección de datos personales", en Ornelas Nuñez, Lina y Piñar Mañas, *La protección de datos personales en México*, México, México, Tirant lo Blanch Monografías, 2013. P 54, disponible en *https://www.tirant.com/mex/libro/la-proteccion-de-datos-personales-en-mexico-9788490336793.*

A continuación se presenta un breve análisis de los principios del tratamiento de datos personales contenidos en la LFPDPPP a la luz del procesamiento automatizado de datos:

a. Licitud.

La licitud es la obligación que el responsable tiene respecto al apego a la legalidad de conformidad con las disposiciones legales aplicables. El numeral 7 de la LFPDPPP establece que la obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos. El tratamiento de los datos personales debe respetar en todo momento la confianza que se deposita en ellos para uso[103] en consideración a la confianza depositada en el responsable y a la expectativa razonable de privacidad del titular.

b. Consentimiento.

Se entiende por consentimiento al elemento de existencia en algunos actos jurídicos, que se integra por el acuerdo de dos o más voluntades[104]. De conformidad con el Artículo 1803 del Código Civil Federal, el consentimiento puede ser expreso verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos, y puede ser tácito al resultar de hechos o de actos que lo presupongan o que autoricen a presumirlo.

El Artículo 3, fracción IV de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares considera como consentimiento a la "manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos." A su vez, en el numeral 8, se estipula que todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la ley. Dicha legislación reconoce los mismos medios

[103] ¿Cómo ejercer el derecho a la protección de datos personales?, consultado el 20 de octubre, disponible en http://inicio.ifai.org.mx/SitePages/Como-ejercer-tu-derecho-a-proteccion-de-datos.aspx?a=m1g.
[104] Adame Goddard, Jorge, *Diccionario Jurídico Mexicano*, Universidad Nacional Autónoma de México, México, 1983, t. II, p. 255.

de expresión de la voluntad que el Código Civil Federal para la manifestación del consentimiento expreso.

De igual forma, el numeral 17 de la LFPDPPP, señala que el titular de los datos otorga un consentimiento tácito para el tratamiento de sus datos, cuando habiéndose puesto a su disposición el aviso de privacidad, no manifiesta su oposición. Para dar cumplimiento a lo anterior, el responsable deberá poner el aviso de privacidad a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.

Por su parte, el artículo 9, establece la obligación de obtener el consentimiento del titular, de forma inequívoca, expresa y por escrito a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca siempre que se recopile o se trate datos personales sensibles.

El numeral 12 de tal ordenamiento señala que el tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. En el caso de que se prevea tratar a los datos con fines distintos, se tiene la obligación de recabar nuevamente el consentimiento del titular. Además, dicho ordenamiento legal establece la potestad de revocar el consentimiento en cualquier momento sin que se le atribuyan efectos retroactivos.

Este principio recae en el derecho del titular de los datos para permite decidir de manera informada, libre, inequívoca y específica qué información se desea compartir con otras personas y para qué finalidades. Lo anterior está regulado por el numeral 12 del Reglamento de la LFPDPPP y conlleva que la elección libre sea aquella en la que no se afecte la manifestación de la voluntad a través del error, mala fe, violencia o dolo.

En los artículos 37 de la LFPDPPP y 70 de la LGPDPPSO se establecen excepciones al principio del consentimiento cuando la transferencia esté prevista en una Ley o Tratado en los que México sea parte; sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia; para la prevención o el diagnóstico médico, la prestación de asistencia

sanitaria, tratamiento médico o la gestión de servicios sanitarios; sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial o para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.

En el caso de que se transfieran datos a un tercero que a cuenta y nombre del responsable, administre un sistema biométrico, ésta se considerará como una remisión, no una trasferencia, por lo cual no es necesario informarla a través del aviso de privacidad ni el consentimiento del titular para que ello suceda.[105]

La transferencia también puede tener lugar sin consentimiento expreso del titular en el caso de que sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas o cuando sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero.

c. Información.

El principio de información, contenido en el numeral 23 del Reglamento de la LFPDPPP hace referencia a la obligación del responsable de dar a conocer al titular la información relativa a la existencia y características principales del tratamiento a que serán sometidos sus datos personales. Tal información debe brindarse por medio del aviso de privacidad y de conformidad con la legislación vigente. Para que el principio de información se observe, es necesario considerar aspectos como la transparencia frente al titular de los datos y la respuesta del responsable, en los términos que marca la ley además de cumplir con los lineamientos referentes al aviso de privacidad.

El aviso de privacidad es el medio por el cual se pone de manifiesto la información que se recaba y los fines con la que se usará. El artículo 24 del Reglamento de la LFPDPPP establece la obligación de que sea sencillo, expresado

[105]Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, "Guía para el tratamiento de datos biométricos", *op. cit*., p. 44.

en lenguaje claro y comprensible, con información necesaria, y contar con una estructura y diseño que facilite su entendimiento. El siguiente numeral del mismo ordenamiento señala que su difusión podrá realizarse a través de cualquier medio, siempre y cuando garantice que el titular tuvo acceso a él, ya sea por formatos físicos, electrónicos, medios verbales o cualquier otra tecnología.

Entre la información que debe brindarse se considera si existe un fichero de datos, es necesario especificar donde se almacenará, los fines del tratamiento de los datos, quienes tendrán acceso a la información, así como las consecuencias del tratamiento de su información, es decir, el alcance al que se puede llegar mediante todo el proceso de recopilación, almacenamiento, procesamiento, traslado a terceros, etc.

En el caso de que los datos sean tratados a partir de métodos de procesamientos y analítica de big data, también debe hacerse del conocimiento de los titulares, así como la información que puede o pretende allegarse luego de su procesamiento. Cuando se lleve a cabo una desindexación, debe especificarse los métodos y la eficacia, de igual forma con los otros medios de encriptación de información y procesos de seguridad, siempre y cuando esto no vulnere su protección, especificar los procedimientos para ejercer los derechos ARCO, así como el responsable ante quien se debe acudir, los procesos y dirección para hacerlo. De igual manera, cuando se realice un proceso de borrado de datos también debe indicarse de qué forma se realiza y dar una garantía de cumplimiento de dicha obligación.

d. Calidad.

El principio de calidad de los datos refiere a la veracidad y la actualización de los datos para que sean correctos conforme a la realidad con el objeto de que no se altere la veracidad de la información. Para dar cumplimiento al principio, numeral 36 del Reglamento señala que el responsable debe procurar que los datos personales que trate sean exactos, completos, pertinentes, correctos y actualizados. De igual

forma, es obligación del responsable, adoptar medidas para que los datos se sujeten al principio de calidad para que el titular no se vea afectado a falta de tal situación.

Además de lo anterior, el principio de calidad implica que el tiempo que el responsable conserve los datos no debe exceder más allá de lo necesario para el cumplimiento de los fines que justificaron su tratamiento. El numeral 39 del mismo ordenamiento señala que es obligación del responsable demostrar que los datos personales se conservan o, en su caso, bloquean, suprimen o cancelan cumpliendo los plazos previstos en la ley. Una vez que se haya cumplido la finalidad para la cual se proporcionaron los datos, el tratamiento deja de ser necesario y, por lo tanto, las empresas deben cancelarlos.

e. Finalidad.

En el artículo 12 de la LFPDPPP se expresa que las finalidades del tratamiento que se le dé a los datos, deben obedecer solamente a las establecidas en el aviso de privacidad. A su vez, el numeral 40 del reglamento señala que estas, deberán ser determinadas, claras, sin lugar a confusión y de manera objetiva se especifica para qué objeto serán tratados los datos personales.

El responsable tiene la obligación de distinguir entre las finalidades que son necesarias para la relación jurídica entre el responsable y el titular, y entre las que no lo son. Tal diferencia debe estar plasmada en el aviso de privacidad, por lo cual, el titular tiene el derecho de otorgar, negar o revocar su consentimiento, así como oponerse para el tratamiento de sus datos personales para éstas últimas, sin que ello tenga como consecuencia la conclusión del objeto del tratamiento de los datos que dio origen a la relación jurídica.

f. Lealtad.

El principio de lealtad se estable como la obligación de tratar los datos personales privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados

conforme a lo que acordaron las partes, de conformidad con el numeral 7 de la LFPDPPP.

Este principio conlleva la prohibición del empleo de medios engañosos o fraudulentos para recabar y tratar datos personales. En el artículo 44 del Reglamento se prevé que por esto último se entiende la existencia de dolo, mala fe o negligencia en la información proporcionada por parte del responsable al titular sobre el tratamiento o cuando las finalidades no son las informadas en el aviso de privacidad.

g. Proporcionalidad.

El artículo 45 del Reglamento contempla al principio de proporcionalidad como aquel que establece que sólo podrán ser objeto de tratamiento los datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las que se hayan obtenido para dar cumplimiento a lo anterior, se estará sujeto al criterio de minimización en el que se establece que el responsable deberá realizar esfuerzos razonables para que los datos personales tratados no sean excesivos y por el contrario, sean los mínimos necesarios de acuerdo con la finalidad del tratamiento que tenga lugar.

h. Responsabilidad.

El principio de responsabilidad, contemplado en la fracción III del artículo 3 de la LFPDPPP se entiende como la obligación de velar y responder por los datos personales que se encuentren bajo la custodia de cualquier persona física o moral de carácter privado que decida sobre su tratamiento ya sea que se encuentren en posesión del responsable o que se hayan transferido a un encargado, aunque este último se encuentre o no en territorio mexicano, de conformidad al Artículo 47 del Reglamento de la ley.

Este principio requiere que las organizaciones analicen el tipo de datos a los que se realiza el tratamiento, con qué finalidades lo hacen y qué tipo de operaciones se llevan a cabo. A partir de este conocimiento deben determinar de forma explícita

la manera en la que aplicarán las medidas que la legislación prevé, asegurándose de que sean las adecuadas para cumplir con el Principio de Responsabilidad.

El Considerando 74 del RGPD describe al Principio de Responsabilidad Proactiva como la obligación que recae en el responsable del tratamiento de datos para que éste aplique las medidas oportunas y eficaces. El Artículo 5 del capítulo II concerniente a los Principios relativos al tratamiento de datos establece que el responsable del tratamiento debe ser capaz de demostrar que cumple lo dispuesto en el apartado, relativo a los principios de licitud, lealtad y transparencia; limitación de la finalidad; minimización de datos; exactitud; limitación del plazo de conservación; integridad y confidencialidad.

Entre los instrumentos internacionales más relevantes para los principios del tratamiento de datos personales se encuentra:

Las Recomendaciones de la Organización para la Cooperación y el Desarrollo Económico realizadas a través de las Directrices relativas a la protección de la privacidad y flujos trasfronterizos de los datos personales, adoptada el 23 de septiembre de 1980 señala los principios de limitación de recogida; de calidad de los datos; de especificación de los fines; de limitación de uso; de salvaguardia de la seguridad; de transparencia; de participación individual y el principio de responsabilidad. Si bien, los nombres de dichos principios no son una réplica de los encontrados en la legislación nacional, versan sobre los mismos objetivos y la diferencia principal radica en que las Directrices de las OCDE no contemplan a la Confidencialidad como un principio.

El Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal del 28 de enero de 1981, también conocido como Convenio 108 del Consejo de Europa, enuncia principios igualmente equivalentes a los contemplados en la LFPDPPP sin un reconocimiento expreso como principios a los referentes al consentimiento, a la responsabilidad, y a la confidencialidad.

El Marco de Privacidad del foro de Cooperación Económica Asia-Pacífico, también conocido como APEC o Sistema de Reglas de Privacidad Transfronteriza (*Cross-Border Privacy Rules CBPRs*) reconoce los principios de prevención de daños; aviso; límites a la recolección; propósito del uso de información personal; elección; integridad de la información personal; medidas de seguridad; acceso y corrección; y responsabilidad.

Los Estándares Internacionales sobre Protección de Datos Personales y Privacidad, llevada a cabo el 5 de noviembre de 2009, conocidos como la Resolución de Madrid reconocen los mismos principios que la legislación nacional de la materia.

La Directiva 95/46/CE del Parlamento Europeo y del Consejo, del 24 de octubre de 1995, relativa a la Protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[106] señalaba en su considerando 25 los principios para el tratamiento, en los que a diferencia de la ley nacional, no reconocía al principio de responsabilidad. No obstante, este instrumento hacía una mención expresa a la obligación de proteger los datos, tanto al tratamiento automático de datos como a su tratamiento manual. Esta legislación es el antecedente directo del RGPD que actualmente incorpora a la responsabilidad proactiva como uno de los ejes de la protección de los datos.

El principio de responsabilidad proactiva, hallado en el considerando 74 del RGPD consiste en la obligación impuesta al responsable del tratamiento de los datos, para que de conformidad con lo establecido en la legislación, aplique las medidas oportunas y eficaces para el tratamiento de los datos. Esta obligación se encuentra aparejada al deber de demostrar que tales medidas son eficaces, tomando en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas físicas.

[106]Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, derogada por el Reglamento 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Aunado a lo anterior, el Reglamento General de Protección de Datos Personales de la Unión Europea, incorpora los derechos a no ser sujeto de toma de decisiones automatizadas y a la protección de datos desde el diseño y por defecto. El principio de protección de datos por defecto o privacidad desde el diseño implica que el responsable debe adoptar medidas que garanticen la protección de los datos en cumplimiento con la legislación, desde que se diseñe una empresa, producto, servicio o actividad.

2.7 Deberes de seguridad y confidencialidad.

La LFPDPPP, reconoce los deberes de seguridad y confidencialidad de los datos. Este último, se regula en el artículo 21 del mismo ordenamiento y plantea que quienes intervengan en el tratamiento de datos personales deberán guardar confidencialidad. Estas obligaciones subsisten aunque se haya finalizado la relación con el titular o con el responsable de los datos.

El deber de seguridad está contemplado por el numeral 19 del mismo ordenamiento y establece que el responsable tiene la obligación de mantener medidas de seguridad administrativa, técnicas y físicas con el fin de proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. Para la implementación de las medidas de seguridad, debe considerarse factores como el riesgo, la sensibilidad de los datos, el desarrollo tecnológico y las posibles consecuencias para los titulares.

El responsable debe establecer por lo menos las mismas medidas de seguridad que mantengan para el manejo de su información, puede cumplir esta obligación por sí o contratar a una persona física o moral para tal fin, para esto, debe considerar el número de titulares; las vulnerabilidades previas; el riesgo con respecto al valor potencial de los datos para un tercero, y cualquier otro factor que puedan incidir en el nivel de riesgo, de conformidad al artículo 60 del Reglamento.

En relación a lo anterior, el responsable deberá tomar acciones para la seguridad de los datos personales entre las que se encuentran, realizar un inventario de datos personales y de los sistemas de tratamiento; determinar las

funciones y obligaciones de las personas que traten datos personales a quienes se deberá capacitar para tal efecto; establecer medidas de seguridad aplicables, analizar y elaborar un plan para implementar aquéllas faltantes que resultan necesarias para la protección de los datos personales; realizar revisiones o auditorías y un registro de los medios de almacenamiento de los datos personales, en consideración al artículo 61 del Reglamento.

El numeral 62 del mismo ordenamiento prevé que los responsables deberán realizar actualizaciones en la relación de las medidas de seguridad cuando se vulneren los sistemas de tratamiento, se modifiquen las medidas o procesos de seguridad y exista una alteración a los datos personales.

Las vulneraciones a los datos ocurren a través de acciones no autorizadas que van desde la pérdida o destrucción, robo, extravío o copia, uso, acceso, tratamiento o modificación de los datos. Para el caso del manejo de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.

2.8 Transferencia de datos a terceros.

La fracción XIX del artículo 3 de la LFPDPPP reconoce como transferencia de datos a “toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento”. Por su parte, el artículo 36 de la LFPDPPP establece que la pretensión de su transferencia, debe comunicarse al titular de los datos, mediante el aviso de privacidad, que a su vez, debe contener una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, sin importar si la transmisión se realiza a terceros nacionales o extranjeros.

La legislación nacional estima la obligación del tercero receptor de asumir las mismas obligaciones que correspondan al responsable que transfirió los datos y usar los datos para las finalidades a las que el titular sujetó su tratamiento. Esta obligación es similar a la contenida en el artículo 44 del RGPD correspondiente al Principio general de las transferencias en el que se estima que sólo se realizarán transferencias de datos a un tercer país u organización internacional si el

responsable y el encargado del tratamiento cumplen las condiciones establecidas a fin de asegurar que el nivel de protección de las personas físicas garantizado por el Reglamento no se vea menoscabado.

Entre las obligaciones del responsable que transfiere datos personales, se encuentran las de formalizar la transferencia mediante algún instrumento jurídico que permita demostrar que el responsable comunicó al tercero receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales y se prevean al menos las mismas obligaciones a las que se encuentra sujeto el responsable que transfiere los datos, así como las condiciones en las que el titular consintió el tratamiento de sus datos personales. En el caso del receptor que reciba datos personales de un responsable del sector privado, deberá probar que la transferencia se realizó conforme a lo que establece la LFPDPPP y su Reglamento y asumir las mismas obligaciones que corresponden al responsable que transfirió los datos, incluyendo el deber de confidencialidad.

El Convenio 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, hecho en Estrasburgo, Francia, el veintiocho de enero de 1981, es uno de los reguladores más atinados en la materia. La relación de México frente al Convenio ha tenido lugar, en un inicio a través de la solicitud de adhesión al Convenio, enviada al Consejo de Europa el 25 de agosto de 2017, que a su vez dio origen a una evaluación realizada a las leyes nacionales en las que se determinó que el Estado contaba con una legislación suficiente que garantizara la protección a los datos bajo los estándares necesarios para llevar a cabo las transferencia en un nivel igual al de los estados miembros.

Con el fin de evitar que las transferencias internacionales de datos tengan como resultado eludir las legislaciones, el Convenio refiere que el flujo trasfronterizo de datos personales “sólo podrá efectuarse si dicho Estado u organización garantiza un nivel de protección adecuado a la transferencia de datos prevista.” Por lo tanto, si el Estado no es miembro del convenio, debe comprobar que cuenta con mecanismos suficientes para brindar una protección amplia, esto supone un medio de protección de los datos a nivel internacional.

Otro instrumento a considerar son las Directrices relativas a la protección de la privacidad y flujos transfronterizos de datos personales, en forma de Recomendación del Consejo de la Organización para la Cooperación y el Desarrollo Económico, fueron adoptadas y entraron en vigor el 23 de septiembre de 1980, lo que dio lugar al primer instrumento enfocado a la protección de la privacidad en relación con los flujos transfronterizos de datos personales en un plano internacional.

Las Directrices de Privacidad compilan una serie de “principios básicos”, en su momento, fueron creadas con el fin de servir de fundamento para la legislación en aquellos países que todavía no dispongan de ella“, además, en tal ordenamiento se considera a los cambios tecnológicos como una de las motivaciones para su consenso, por lo cual, aun es aplicable. Su ámbito de aplicación incide tanto del sector público como del privado y abarcan temas que abarcan principios básicos de aplicación general, principios básicos de aplicación internacional: libre circulación y restricciones legítimas, el proceso de implantación nacional y de cooperación internacional.

El reconocimiento a Estados y a empresas privadas mediante resolución del Consejo de Europa o a través de estándares internacionales, plantea una alternativa segura a la hora de elegir empresas proveedoras de servicios digitales, lo que a su vez otorga una alternativa confiable para la elección de proveedores con los que se llevará a cabo transmisión o tratamientos de datos.

2.9 La eficacia de la norma jurídica frente al tratamiento automatizado de los datos en las plataformas digitales.

Derivado del análisis de los principales instrumentos jurídicos que regulan la protección de la privacidad y de los datos personales, podemos observar que el marco jurídico nacional e internacional es sólido respecto a la protección contemplada en tales normas. No obstante, las leyes reconocen lo que en una sociedad es jurídicamente aceptable y exigible, sin embargo, la transformación de

la realidad no es inmediata a la emisión de leyes ni mucho menos automática y la existencia de un orden normativo no es suficiente para lograr su cumplimiento.

Podemos considerar dos obstáculos principales para ello: la limitación innata del derecho frente a la modificación de la realidad que pretende regular y el escaso poder que los Estados tienen en el ciberespacio.

Hume es bastante claro al proponer la "imposibilidad de la deducción de juicios cuya cópula es un *debe* a partir de premisas cuya cópula es un *es*"[107]. Esto plantea la imposibilidad de obtener deducciones de juicios normativos, de premisas fácticas. Lo anterior conlleva a concluir que de una realidad de hecho, resulta insostenible pretender hacer un cambio por medio de un juicio de valor o normativo[108]. La limitación del derecho, en un entorno fáctico es uno de los obstáculos más grandes a sortear no sólo en el derecho informático, sino en todas las áreas que las normas jurídicas pretenden regular.

En el mismo sentido, Federico César Lefranc Weegan estima que el derecho tiene un papel simbólico para la sociedad que se funda en la confianza de que a partir de él, las cosas pueden ir mejor[109]. Aunado a lo anterior, podemos considerar que las sanciones contenidas en las legislaciones, son sólo un instrumento que funge con una función disuasoria frente a su incumplimiento.

Es comprensible que la regulación de conductas en el ciber espacio enfrente por lo menos los mismos problemas que se hallan fuera de él. Por consiguiente, nos hallamos ante las limitaciones tradicionales de la eficacia de la norma jurídica y además, frente a un entorno en el que las posibilidades de las actividades humanas, se exponencian a través de la tecnología.

---

[107] Widow Lira, Felipe, "La ley de Hume en Hume: la discusión de la interpretación analítica de Treatise III, 1, i", *Anales del Seminario de Historia de la Filosofía,* vol. 32, num. 2, 2015, p. 417, disponible en *https://revistas.ucm.es/index.php/ASHF/article/view/49971* (última fecha de consulta el 19 de octubre de 2019).

[108] *Idem.*

[109] Lefranc Weegan, Federico César, *Terra Incognita Bases para una política criminal pro persona en la sociedad digital*, México, Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación, 2015, p.9.

En el ciberespacio se han gestado relaciones humanas a gran escala que plantean una nueva estructura, lo que puede desembocar en la existencia de una especie de Macro Estado Virtual[110]. Federico César Lefranc Weegan considera que existen dos características que afectan la posibilidad de la protección de los derechos de las personas en el ciberespacio: la primera surge del hecho de que el Internet es el producto de corporaciones privadas y por consiguiente, escapa a los alcances del derecho público. La segunda razón es que su regulación obedece al *common law*, lo que genera una disparidad frente al modelo del derecho continental.[111]

Aunado a ello, las plataformas digitales dotan de una nueva dimensión a las interacciones entre humanos e incluso, humano-maquina, lo cual dificulta la regulación bajo un marco normativo que obedezca las mismas reglas del mundo físico. En este sentido, Marshall McLuhan estima que la aceleración de la información, provoca que los espectadores se convierten en productores, en lugar de consumidores y la posibilidad de participación pública se convierte en una especie de imperativo tecnológico en la que "Si se puede hacer, se tiene que hacer"[112]. Lo anterior plantea que la técnica avanza en la medida de lo posible y las restricciones normativas podrán ser disuasorias o punitivas, pero estas no impedirán que se desarrolle la técnica ni que cada vez sean más los partícipes de ello.

En suma, la salvaguarda de la privacidad y de los datos personales que se procesan a través de plataformas digitales y herramientas de procesamiento automatizado, requieren de la incorporación de una perspectiva diferente a la usada en los procesos tradicionales para hacer frente a las amenazas y riesgos que sólo son salvables a través de un cambio de paradigma sobre su protección y los medios para lograrla.

---

[110] *Ibidem* p. 27.
[111] *Idem.*
[112] Marshall McLuhan, Herbert. “At the moment of Sputnik the planet became a global teather in wich there are no spectators bur only actors”, *Journal of Communication*, invierno de 1974, vol. 24, num. 1, p. 57, consultado el 24 de septiembre, disponible en https://academic.oup.com/joc/article/24/1/48/4553567.

Derivado de esto, el tratamiento de los datos personales y la privacidad alcanzan una nueva dimensión que requiere el fomento de una interoperabilidad entre los diferentes actores que intervienen en el procesamiento de datos a través de plataformas digitales e incluir a las herramientas técnicas disponibles para lograrlo.

Capítulo 3

Recomendaciones

Capítulo 3. Recomendaciones

La gobernanza de los datos implica una colaboración entre los diferentes actores involucrados en el tratamiento de los datos. Para Bernard Marr, las políticas de gobernanza de los datos "hacen referencia a la gestión y cuidado global de los datos, que incluye su usabilidad e integridad y su seguridad".[113] Lograrlo conlleva fomentar la adquisición de conocimientos y habilidades que promuevan la participación de todos los actores involucrados.

A su vez, el tratamiento responsable de la información supone la colaboración entre las diferentes partes que intervienen y los expertos en estos desafíos. Esto conlleva incluir a la sociedad civil, expertos en seguridad de la información, investigadores, empresas privadas, especialistas en ética y al público en general[114]. En suma, su incorporación es multifactorial y requiere de la contribución de todos los involucrados.

La orden ejecutiva, titulada *Accelerating America's Leadership in Artificial Intelligence* o Acelerar el liderazgo de Estados Unidos en inteligencia artificial, por su traducción al español, contiene cinco pilares básicos en relación con la expansión de los esfuerzos de investigación de la IA en Estados Unidos. Estos pilares lo son la investigación y desarrollo; infraestructura: gobernanza; formación y el compromiso internacional.[115] Entre las medidas destaca la gobernanza, en la que se considera establecer normas éticas y seguridad para el uso de inteligencia artificial.

A su vez, la recomendación de la OCDE sobre los principios de Inteligencia Artificial es un lineamiento no vinculante para orientar al tratamiento ético. Se

---

[113] Marr, Bernard, *Data Strategy: Cómo beneficiarse de un mundo de Big Data, Analytics e internet de las cosas*, Trad. Ramia Inés y Jimenez Alicia, s.l.i., Editorial Teell, 2018.
[114] Brundage, Miles, *et al*. "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation", Future of Humanity, Institute University of Oxford, Centre for the Study of Existential Risk, University of Cambridge, Center for a New American Security, Electronic Frontier Foundation, OpenAI, febrero de 2018, p.52, disponible en *https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf* (última fecha de consulta octubre de 2018).
[115] "Las Iniciativas de EE UU En Materia de la y el Futuro de los Gobiernos", consultada el 13 de octubre, disponible en *https://www.ma-no.org/es/las-iniciativas-de-ee-uu-en-materia-de-ia-y-el-futuro-de-los-gobiernos.*

presenta como un complemento a los estándares existentes en áreas como privacidad, gestión de riesgos de seguridad digital y conducta empresarial responsable. En palabras de la organización, son "suficientemente prácticos y flexibles como para resistir el paso del tiempo en un campo en rápida evolución" [116]. La recomendación que contiene los principios versa sobre 5 ejes: crecimiento inclusivo, desarrollo sostenible y bienestar; valores centrados en el ser humano y equidad; responsabilidad; transparencia y explicabilidad; robustez, seguridad y protección[117]. Las recomendaciones abarcan políticas públicas, economía, gobernanza, instituciones privadas, ciencias sociales, técnica, formación orientada a derechos humanos.

Entre los ejes de la política de privacidad orientada a la gobernanza de los datos, es menester considerar la formulación de políticas públicas en colaboración con el sector privado y con los especialistas en ciberseguridad, con el fin de prevenir y mitigar los riesgos y hacer uso de las tecnologías informáticas disponibles para brindar una mayor seguridad a la información para fomentar una mayor protección de los datos personales a través de las plataformas digitales, por medio del tratamiento automatizado de los datos.

3.1 Políticas Públicas.

La Unión Internacional de Telecomunicaciones, estima que a finales del 2018, 3 900 millones de personas utilizaban Internet, lo que equivale al 51,2% de las personas de la población mundial. En el caso de los países desarrollados, cuatro de cada cinco personas están en línea.[118] Además del número de personas conectadas actualmente a la red de redes, se espera que se pueda llegar a un índice de

[116] Organización para la Cooperación y el Desarrollo Económicos, *What are the OECD Principles on AI?*, disponible en *http://www.oecd.org/going-digital/ai/principles/* (última fecha de consulta el 15 de octubre de 2019).
[117] Organización para la Cooperación y el Desarrollo Económicos, *Recommendation of the Council on Artificial Intelligence, op. cit.*
[118]Unión Internacional de Telecomunicaciones, *Informe sobre Medición de la Sociedad de la Información, Resumen analítico 2018,* ITU Publicaciones, 2018, disponible en *https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR2018-ES-PDF-S.pdf (última fecha de consulta el 8 de septiembre de 2019).*

penetración de Internet del 70% de la población mundial para 2023 y del 75% para 2025.

La influencia de la penetración de la digitalización en México se refleja en la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares, realizada por el Instituto Nacional de Estadística y Geografía[119] de manera anual en habitantes del territorio mexicano, mayores de 6 años. El estudio revela que en el 2018 se registraron 74.3 millones de usuarios en todo el territorio mexicano y el 90.5 por cierto de las personas que viven en México se conectan a la red para acceder a contenidos de entretenimiento, mientras que el 90.3 lo hace para comunicarse, el 86.9 para obtener información, el 83.6 para capacitación o educación, el 78.1 para descargar contenidos audiovisuales y el 77.8 para acceder a redes sociales. A su vez, se estima que el 92.7 accede a la red a través de su teléfono móvil, los siguientes dispositivos más usados son las computadoras portátiles con el 32.6%; las computadoras de escritorio con el 32%; las tabletas con el 17.8%; televisores inteligentes con el 16.6% y por último los que se conectan a través de una consola de videojuego con el 6.9%. [120]

Por otra parte, la ENAID o Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales, levantada por el Instituto Nacional de Geografía y Estadística es el único instrumento gubernamental estadístico que se cuenta para conocer el grado de conocimiento del derecho de protección de datos personales y de los mecanismos para su protección. La encuesta fue realizada entre los años 2015 y 2016 a personas mayores de 18 años con residencia en viviendas particulares en áreas urbanas.[121]

El instrumento revelo que entre las principales preocupaciones del uso indebido de los datos que han proporcionado a redes sociales se encuentra en

---

[119] Instituto Nacional de Estadística y Geografía, *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares,* 2018, disponible en *https://www.inegi.org.mx/programas/dutih/2018/default.html#* (última fecha de consulta el 5 de octubre de 2019).

[120] *Idem.*

[121] Instituto Nacional de Geografía y Estadística, *Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales (ENAID),* p. 8, disponible en *https://www.inegi.org.mx/programas/enaid/2016/* (última fecha de consulta el 17 de marzo de 2019).

primer lugar el uso indebido de su dirección con un 87.7% de personas que manifestaron preocupación, seguido del 86.5 % preocupados por el uso indebido de su número de celular y el 84.3% por el uso indebido de su nombre[122].

A pesar de que un gran número de encuestados han manifestado un alto grado de preocupación por el uso indebido de sus datos personales en las plataformas digitales, particularmente de las redes sociales, sólo el 32.7% de la población dice que las instituciones que tratan sus datos le han proporcionaron un aviso de privacidad[123] y sólo el 1.4% de la población ha presentado una queja por uso indebido de sus datos personales[124]. La situación es aún más sorprendente ya que de las quejas presentadas, sólo el 10.1 % se realizó ante el INAI.[125]

Por otra parte, el Estudio de Protección de Datos Personales entre Usuarios y Empresa reveló información relevante sobre el conocimiento sobre datos personales que tiene una muestra de usuarios y empresas. Entre los datos más relevantes se halla que el 28% de las empresas evaluadas no pudieron definir lo que es un dato personal; el 44% no cuenta con suficiente conocimiento de la LFPDPPP; 5 de cada 10 empresas no tienen suficiente conocimiento de los derechos ARCO y estiman que el principal obstáculo para implementar acciones es el desconocimiento de la ley, en este sentido, el 41% declara un desconocimiento parcial y 22% un desconocimiento total sobre la ley; además el 74% considera que no se ha difundido apropiadamente el impacto de ley en México. [126]

En atención a lo presentado en el primer capítulo, podemos dimensionar que la cantidad y la calidad de la información recopilada a través de las plataformas digitales va más allá del nombre, la dirección, el teléfono o de otros datos que se requieren para el registro o acceso a tales plataformas. No obstante, la encuesta

[122] *Ibidem*, p.7.3.
[123] *Ibidem*, p.7.8.
[124] *Ibidem*, p.7.14.
[125] *Idem.*
[126] Asociación Mexicana de Internet, Estudio de Protección de Datos Personales entre Usuarios y Empresas realizado por la Asociación Mexicana de Internet sobre una base de 734 usuarios de plataformas digitales y 187 empresas evaluadas, AMIPCI, consultado el 11 de junio de 2019, disponible en https://www.asociaciondeinternet.mx/es/component/remository/func-startdown/19/lang,es-es/?Itemid= consultado el 6 de mayo de 2019.

ENAID no contempla el análisis del grado de conocimiento de los ciudadanos y por supuesto, tampoco el grado de su preocupación respecto al tratamiento indebido de la información recopilada por las plataformas sobre sus hábitos, preferencias e intereses.

Lo anterior representa sesgos de la encuesta ENAID respecto al conocimiento con el que cuentan los ciudadanos sobre el manejo de su información a pesar del elevado número de internautas en México y la naturalidad con la que aspectos como la comunicación, entretenimiento y acceso a información suceden a través de internet. Aunado a esto, la encuesta fue realizada en una muestra de población urbana, lo que deja fuera el análisis del grado de conocimiento de las poblaciones rurales de nuestro país. Ambas cuestiones representan sesgos para un diagnóstico efectivo y general, de la situación, aunado a que no existe otra encuesta que abarque los mismos rubros y por ello no puede compararse el avance de las políticas públicas de la materia.

No obstante, los datos que se muestran evidencian un alto grado de preocupación por parte de la población derivado de la desconfianza del manejo de sus datos, un reducido número de quejas, un acercamiento pobre ante la autoridad garante de la materia y por supuesto, esto exterioriza la necesidad de reforzar las políticas públicas destinadas a aumentar el conocimiento de las personas respecto a los derechos de protección de sus datos personales y las demás prerrogativas que giran en torno a este, así como los procesos para garantizar su protección.

Además, se observa que el sector privado cuenta con un escaso conocimiento de la ley de la materia y de los derechos ARCO, esto supone un claro obstáculo para acercar medidas dirigidas hacia el respeto de los derechos de protección de datos y de privacidad.

La participación ciudadana, de empresas privadas, de asociaciones civiles, de industria y de academia, resulta relevante para fomentar un enfoque preventivo en el desarrollo de software seguro, en el uso de herramientas informáticas que promuevan una mayor protección a los datos, de incorporación de protocolos

seguros el tratamiento de la información e incluso una presión en el mercado para optar por las empresas que cumplan con el respeto de los derechos de privacidad, protección de datos y los que concurren con ellos en su ejercicio.

A través del presente trabajo propongo que se contemple la puesta en marcha de políticas públicas que abarquen 3 ejes principales: la prevención, la educación y la socialización.

Prevención

La cultura de la prevención de las vulneraciones a los derechos de privacidad es sólida en la legislación pues se reconoce una serie de medidas tendientes a prevenir que suceda. Sin embargo, como se ha planteado con anterioridad, la simple existencia de la legislación, no conlleva su cumplimiento de forma automática. En este sentido, es menester fortalecer los mecanismos que acerca el acercamiento con las empresas y en especial con las plataformas digitales para fomentar su cumplimiento.

Entre las implicaciones del uso de programas de procesamiento automatizado de datos se reconocen tres implicaciones de alto nivel en relación con las posibles amenazas que conlleva su uso: la posibilidad de expandir las amenazas existentes; la de introducir nuevas amenazas y la de alterar el carácter típico de las amenazas[127]. Por otra parte, la automatización conlleva el manejo de información a una escala exponencial y las características como la velocidad o la facilidad de tratar a los datos, también instauran una ventaja al momento de vulnerarlos o acceder a ellos.

La Agencia Española de Protección de Datos define a la amenaza como "cualquier factor de riesgo con potencial para provocar un daño o perjuicio a los interesados sobre cuyos datos de carácter personal se realiza un tratamiento"[128] y

[127] Brundage, Miles, *op. cit*., p. 18.
[128] Agencia Española de Protección de datos, *Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD, de la Agencia Española de Protección de datos*, p. 3, disponible en *https://d3t4nwcgmfrp9x.cloudfront.net/upload/AnalisisDeRiesgosRGPD.pdf* (última fecha de consulta el 8 de agosto de 2019).

considera que puede haber tres tipos de amenazas correspondientes al acceso, modificación o eliminación provenientes de un tratamiento ilegítimo o no autorizado de los datos[129], lo que a su vez vulneraría la confidencialidad, integridad y disponibilidad de los datos, respectivamente.

A diferencia de las amenazas, los riesgos son "la combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas"[130]. Los riesgos se miden en consideración a la "probabilidad de materializarse y el impacto que tiene en caso de hacerlo."[131] Si bien, el deber de hacer frente a las amenazas del tratamiento de bases de datos con información personal se reviste de una importancia inherente a la protección de un derecho humano y por sí misma, la incorporación de tecnologías de tratamiento automatizado de datos que facilitan el acceso, almacenamiento, análisis y manejo remoto de la big data, también amplían la posibilidad de vulneración de los ficheros. La transgresión a la seguridad de las bases de datos y por consiguiente, a los datos personales, puede traer aparejada la vulneración al derecho de la privacidad.

Entre los riesgos que inherentemente se adquieren al incorporar a las TIC en cualquier proceso, se encuentran los de vulneración al algoritmo o sistema informático que lo alberga.[132] Esto implica no sólo el acceso a la información sino un nuevo uso a ella que se puede derivar de su analítica, a una escala mayor o incluso un progreso en la sofisticación de estos. Los algoritmos pueden no se encuentran exentos de errores ni mucho menos sesgos que nacen ya sea a partir de su escritura y la intención del programador, del encargado o de los datos que alimenta a tal sistema de cómputo. En el próximo capítulo se abordarán algunos de los mecanismos de protección de datos ahondando en la ley nacional de la materia y la relación con instrumentos internacionales.

La incorporación de una perspectiva humanista en el desarrollo de software que involucra personas, presupone encaminar los procesos a una perspectiva

[129] *Idem.*
[130] *Ibidem* p. 4.
[131] *Ibidem* p. 3.
[132] Brundage, Miles, *op. cit*., p. 53.

orientada a la prevención de violación de los derechos humanos. Recientemente se han creado mecanismos para recolectar información sobre cómo piensan los humanos y cómo resolverían dilemas morales con la finalidad de contar con información que ayude a resolver problemas en la toma de decisiones a través de software de respuesta automática. Entre ellos destaca *Moral Machine*, un sitio web que tiene como objetivo proporcionar una plataforma para construir una imagen de la opinión humana y la apertura a una discusión de los posibles escenarios que desencadenen en una consecuencia moral[133].

La efectiva protección de los datos personales en el ciberespacio atraviesa por retos que van desde lo físico como el contar con una infraestructura que dote a los sistemas informáticos de seguridad y confiabilidad; de la educación de consciencia y empoderamiento del usuario para hacer valer sus derechos y de un marco jurídico que dé certeza a los gobernados y los dote de herramientas para exigir el respeto de sus derechos.

El INAI posee una serie de documentos que coadyuvan a facilitar esto, entre los que destacan herramientas como un generador de aviso de privacidad[134], una guía con respuestas a las preguntas frecuentes[135], un evaluador de vulneraciones[136]. No obstante, un mecanismo para para fomentar que el sector privado tome medidas para prevenir o mitigar problemas, amenazas y riesgos es la creación de incentivos. Las empresas cooperan frecuentemente para resolver problemas de acción colectiva.[137]

---

[133] Moral Machine , *About Moral Machine*, disponible en http://moralmachine.mit.edu/ (última fecha de consulta el 6 de septiembre de 2019).
[134] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *Sistema Generador de Avisos de Privacidad,* disponible en *https://generador-avisos-privacidad.inai.org.mx/* (última fecha de consulta el 17 de octubre de 2019).
[135] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *El ABC del Aviso de Privacidad*, disponible en *http://abcavisosprivacidad.ifai.org.mx/* (última fecha de consulta el 17 de octubre de 2019).
[136] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *Evaluador de Vulneraciones*, disponible en *http://inicio.ifai.org.mx/SitePages/Evaluador-Vulneraciones.aspx* (última fecha de consulta el 15 de octubre de 2019).
[137] Askell, Amanda, *The Role of Cooperation in Responsible AI Development*, p. 19, disponible en *https://arxiv.org/pdf/1907.04534.pdf* (última fecha de consulta octubre de 2019).

Educación

Los datos anteriores exponen una fuerte urgencia de fortalecer la alfabetización digital a través de medidas que permitan el desarrollo de competencias para el uso de dispositivos informáticos de una manera responsable. Una estrategia integral, vislumbra acercar a la población de los medios que le permita detectar posibles riesgos y amenazas a la privacidad, y la potestad de tomar medidas con el fin de disminuirlos. A su vez, es necesario generar una cultura de prevención de incidentes e ilícitos cometidos a través de dispositivos electrónicos.

Lo anterior presupone la creación de políticas públicas que fomenten la inclusión de ciencias sociales en los programas académicos de las ciencias exactas. Esto conlleva el auge de programas encaminados al desarrollo de software, hardware y de innovación tecnológica de cara a los principios de protección de datos, lo que se traduce en un mayor desarrollo de sistemas con privacidad por diseño. También es menester incluir programas académicos que incentiven la innovación tecnológica y la participación en la economía digital con un enfoque de protección de los derechos humanos desde el diseño de las plataformas dogotales y otros sistemas tecnológicos.

Carlos Osorio estima que la sociedad de consumo y el sistema económico de producción ha puesto en una encrucijada al sujeto racional entre la aceptación de sí como objeto, instrumento o artefacto en el sistema artefactual o recabar la capacidad racional, en la que es requerido hoy como un sujeto de racionalidad tecnológica.[138] A su vez, señala la importancia de considerar a los sistemas tecnológicos como una unidad para la enseñanza de la ingeniería desde los enfoques en ciencia, tecnología y sociedad[139].

Al respecto, Graciano González Rodríguez-Arnaíz señala que la demanda de formación humanista, por parte de los tecnólogos se legitima con su preparación

[138] Osorio, Carlos, "La participación pública en sistemas tecnológicos. Lecciones para la educación CTS", *Revista iberoamericana de ciencia, tecnología y sociedad*, Buenos Aires, vol. 2, num. 6, 2005, p. 26, disponible en *http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-36282012000200003&lang=es* (última fecha de consulta el 8 de mayo de 2019).
[139] *Idem.*

para que sean capaces de involucrarse en las tareas propias de una sociedad de personas.[140] Esto presupone una mayor adecuación de la currícula estudiantil de los profesionales en desarrollo de software y sistemas informáticos, así como los tomadores de decisiones en el desarrollo de estas herramientas entre las políticas públicas encaminadas a mejorar la educación de los jóvenes.

Socialización

Entre los retos que el Estado enfrenta se encuentran los de mejorar el nivel de conocimiento general sobre el derecho de protección de datos personales; el mecanismo para solicitar la intervención de la autoridad ante una posible vulneración; así como la confianza de la ciudadanía en los mecanismos con los que cuenta para exigir el respeto a sus derechos a través de la socialización de los procedimientos de habeas data. Esto conlleva en un primer momento, lograr que el ciudadano se reconozca como dueño de sus datos personales y cuente con la información suficiente para entrever los efectos del tratamiento de sus datos en manos de terceros.

Es necesario además, que los usuarios conozcan sus derechos y la forma de ejercitarlos, que las autoridades se encuentren preparadas para dar seguimiento a los procesos que se deriven de la aplicación de la norma en un ámbito digital, se cuente con mecanismos que permita sancionar a los infractores y se asegure una reparación del daño para los afectados, así como medidas que impidan la repetición de la conducta violatoria de derechos humanos.

Una de las herramientas que el INAI pone a disposición de los usuarios es la Guía para prevenir el robo de identidad[141] que brinda información sobre el robo de identidad para reducir el riesgo de que esto suceda, promueve el conocimiento de

[140] González Rodríguez-Arnaíz, Graciano, "El imperativo tecnológico una alternativa desde el humanismo", *Cuadernos de bioética*, España, Vol. 15, Num. 53, 2004, p. 37, disponible en *http://aebioetica.org/revistas/2004/15/1/53/37.pdf* (última fecha de consulta el 9 de octubre de 2019).
[141] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *Guía para prevenir el robo de identidad, p. 5,* disponible en *http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Prevenir_RI.pdf* (última fecha de consulta el 7 de agosto de 2019).

los derechos de los titulares y estrategias para disminuir las posibles vulneraciones. Otro de los instrumentos es el ”vulnerómetro[142]” que es una plataforma que a través de preguntas que los usuarios responden, pueden conocer el nivel de vulneración de sus datos personales a los que se encuentran sujetos en relación con sus actividades cotidianas.

Los retos de lograr una socialización de los mecanismos para el ejercicio de los datos personales conlleva el considerar mecanismos más robustos en aras de proteger a poblaciones vulnerables y fomentar el acercamiento al conocimiento de sus derechos por parte de poblaciones con poco o nulo acceso y uso de la tecnología informática.

Los menores de edad son uno de los grupos con mayor exposición a la vulneración de sus derechos. En suma, el fácil acceso a las plataformas digitales puede representar una puerta para la exposición de su intimidad, a la información que los pueda hacer identificables, el acceso de terceros a datos que pongan en riesgo a los menores e incluso la exposición de datos biométricos a través de fotografías y tecnología de reconocimiento facial o el uso indebido de imágenes de los menores para fines que vulneren su dignidad humana.

La protección de este grupo de población exige una colaboración aún más comprometida entre los diversos actores del tratamiento de los datos y de los tutores de los menores para promover un espacio seguro para su desarrollo e interacción en las plataformas digitales. Olivia Andrea Mendoza Enríquez señala que si bien, las leyes de protección de datos no reconocen de manera expresa al principio de interés superior del menor, la aplicación de este principio es de carácter transversal por lo cual puede invocarse para la efectiva tutela de la protección de niños, niñas y adolescentes[143].

---

[142] *Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Vulnerómetro, disponible en https://micrositios.inai.org.mx/vulnerometro/index.php (última fecha de consulta el 7 de agosto de 2019).*

[143]Mendoza Enríquez, Olivia Andrea, “Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento”, *ius Revista del Instituto de Ciencias Jurídicas de Puebla*, México. vol. 12, num. 41. enero-junio de 2018., p. 278.

Considero que en el mismo tenor que los datos biométricos cuentan con una protección especial, el tratamiento de datos de menores de edad debe obedecer a principios especiales para su recopilación y tratamiento. Esto en consideración con un consentimiento expreso de los tutores para su tratamiento, aun en plataformas digitales, una mayor difusión de las campañas del INAI sobre su relevancia e incluso la contemplación de la industria una restricción de hacer uso de la tecnología de analítica de big data para promover cualquier tipo de promoción ante menores de edad. Lo que supone promover un respeto al libre dearrollo de su psique y blindarlos frente al fomento de información que pueda tratarlos más como consumidores y como materia prima del análisi de información que como personas.

3.2 Buenas prácticas y autorregulación.

La participación del sector privado y su influencia en el desarrollo por medio del uso de herramientas de procesamiento automatizado de datos le otorga un papel relevante para fomentar la protección de datos a través de herramientas informáticas. Entre las medidas que este puede tomar, se encuentran la adopción de estrategias de autorregulación y buenas prácticas que no se contrapongan a los derechos de las personas con el objetivo de proteger la intimidad de los usuarios en las plataformas digitales.

Lo anterior implica considerar factores como un aviso de privacidad acorde con la legislación nacional, la capacitación y sensibilización del capital humano de las empresas sobre la responsabilidad que albergan en sus manos, instauración de protocolos de actuación para la salvaguardar los datos de los titulares, protocolos de actuación en caso de vulneración de las bases de datos, así como la adopción de estándares y lineamientos internacionales.

En el 2007, la Comisión de las Comunidades Europeas emitió una comunicación al Parlamento Europeo y al Consejo sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad. En el documento se contempla el término *PET*, en referencia a “un sistema coherente de medidas de TIC que protege el derecho a la intimidad suprimiendo o reduciendo los

datos personales o evitando el tratamiento innecesario o indeseado de datos personales, sin menoscabo de la funcionalidad del sistema de información."[144] El auxilio de este tipo de sistemas puede reducir los riesgos de exposición de la intimidad y aumentar la protección de los datos personales a través de la reducción de la recopilación de los datos.

La relevancia de incluir sistemas informáticos y procesos que contemplen a las tecnologías informáticas destinadas a la protección de datos, aumenta en el sentido de que a través de ello, existe la posibilidad de contrarrestar las amenazas inherentes al uso de las plataformas digitales. Lo anterior se puede atribuir a que los sistemas PET contemplan no sólo procesos, sino también, el auxilio de herramientas que refuerzan la protección de la información y su uso coadyuva al respeto a los principios de protección de los datos.

Sin duda, la implementación y manejo de PETs requiere del compromiso de los responsables del tratamiento que por supuesto, puede ser fomentada a través de la presión de los titulares de los datos que prefieran afianzar relaciones con las plataformas digitales que les brinden una mayor protección y sean transparentes en los alcances y procesos que comprometan sus datos. Esto supone, la reducción de relaciones con aquellas plataformas que no lo hagan. A su vez, la incorporación de PETs requiere de un mayor conocimiento de la industria, del fomento del INAI para su difusión y del aumento de comprensión de los titulares sobre sus derechos, los riesgos del tratamiento, la existencia de estas plataformas y otros aspectos que se abordarán más adelante.

Se requiere adoptar prácticas éticas en aras de garantizar la intimidad de los usuarios de las plataformas digitales y la seguridad de la información en los sistemas informáticos. Uno de los puntos a destacar es la ingeniería de la privacidad

[144] Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad, realizado en Bruselas, 2007, p. 3.

es en sí, una nueva disciplina pues asegurar la privacidad a través de medios eléctricos es innovación[145].

Esto conlleva la aplicación de la privacidad por diseño, la cual promueve una mejora en la eficiencia de procesos a la par de modelos económicos sostenibles a largo plazo[146] a la par que permite el acceso a las ventajas del uso de las TIC sin comprometer la seguridad de los datos de las personas. La privacidad por diseño implica usar un enfoque que permita fijar los requisitos de privacidad mediante prácticas, procedimientos y herramientas con un enfoque metodológico orientado a la gestión del riesgo y de responsabilidad proactiva.[147]

Entre las estrategias que incorporan a la privacidad por diseño se identifican 8 principales a considerar: Minimizar la cantidad de información que se usará; ocultar en lo posible, la información personal que se procese; el procesamiento debe separar los datos personales siempre que sea posible; analizar la información a nivel grupal para restringir el acceso a la mayor cantidad de detalles personales; los interesados deben estar informados cuando se procese información personal; otorgar control a los titulares de los datos sobre su información; debe existir una política de privacidad compatible con los requisitos legales y debe hacerse cumplir; el controlador de los datos debe poder demostrar el cumplimiento de la política de privacidad y los requisitos legales aplicables[148].

La protección de la privacidad, la seguridad de la información en los sistemas informáticos, el desarrollo ético de software y herramientas de analítica así como las opciones accesibles para el libre ejercicio de sus derechos ARCO son algunos de los factores que la industria privada puede atender para fortalecer el respeto a la privacidad y a los datos. La gestión de programas informáticos que no sólo

---

[145] Agencia Española de Protección de Datos*, Guía de Privacidad desde el Diseño, s.l.i, 2019, p.32,* disponible en *https://www.aepd.es/media/guias/guia-privacidad-desde-diseno.pdf* (última fecha de consulta el 1 de agosto de 2019).
[146] *Idem.*
[147] *Idem.*
[148] Hoepman, Jaap-Henk*, "*Privacy Design Strategies", Cuppens-Boulahia N, *et. al*., *ICT Systems Security and Privacy Protection*., vol 428., Springer, Berlin, Heidelberg, 2014, p. 5, disponible en *https://www.cs.ru.nl/~jhh/publications/pdp.pdf* (última fecha de consulta 17 de noviembre de 2019).

consideren a la privacidad de desde diseño, sino también un desarrollo de software en apego al respeto de la dignidad humana en relación con el tratamiento de información personal y la influencia individual y social, suponen una serie de cuestiones a considerar entre las que se encuentran las legales, técnicas, éticas, sociales e incluso económicas.

3.3 Seguridad de los datos.

El desarrollo responsable de Inteligencia Artificial conlleva trabajar en seguridad para mitigar los riesgos asociados y obtener que los sistemas actúen de la forma esperada[149]. Para lograrlo, deben considerarse tanto la seguridad digital, la seguridad física y las políticas de seguridad[150].

La gestión de los riesgos implica una serie de actividades destinadas a controlar la incertidumbre de las amenazas que incluyen la identificación y evaluación del riesgo, así como, las medidas para su reducción o mitigación[151]. En este sentido, es importante identificar amenazas y riesgos derivados de los datos analizados y las herramientas empleadas para minimizar el riesgo. Un Sistema de Gestión de Seguridad de los Datos Personales [SGSDP] tiene como objetivo mejorar la protección de datos personales para el cumplimiento de la legislación y fomentar las buenas prácticas en un marco de trabajo orientado para lograrlo[152].

Las Recomendaciones en materia de Seguridad de Datos Personales[153], del INAI, exhortan la implementación de un Sistema de Gestión de Seguridad de Datos Personales en consideración con un sistema para Planear-Hacer-Verificar-Actuar [PHVA] la protección de los datos personales. Esto implica la consideración de los

---

[149] Askell, Amanda, *op. cit*., p.3.
[150] Brundage, Miles, *et al, op. cit*., p.54.
[151] Agencia Española de Protección de datos, *Guía práctica de Análisis de riesgos en los tratamientos de datos personales sujetos al RGPD*, *op. cit*., p.3.
[152]“ Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales Junio 2015*, p. 7, disponible en *http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf* (última fecha de consulta el 9 de agosto de 2019).
[153] Recomendaciones en materia de seguridad de datos personales, publicadas en el Diario Oficial de la Federación el 30 de octubre de 2013.

factores legales, del modelo de negocio y tecnológicas[154] con el fin de establecer las acciones para la seguridad de los datos. Entre las acciones a llevar a cabo se encuentran las de planear; establecer los objetivos; elaborar una política; establecer funciones y obligaciones de los responsables; elaborar un inventario de los datos personales; analizar el riesgo; identificar las medidas de seguridad; implementar y operar el SGSDP; implementar las medidas; monitorear; realizar revisiones; mejora continua y capacitación[155].

Los controles para lograrlo, albergan el cumplimiento legal; la estructura organizacional de la seguridad; la clasificación y acceso a los activos; la seguridad del personal, fiscal y ambiental; la gestión de comunicaciones y operaciones; el control al acceso; el desarrollo y mantenimiento de sistemas y protocolos de vulneraciones de seguridad[156]. Anteriormente se presentó la relevancia de la incorporación de sistemas PET en el tratamiento de los datos, a continuación se esbozan ejemplos de PET:

- Anonimización automática: Conlleva la guarda de los datos de una manera que sólo permita la identificación de los titulares durante el tiempo necesario y para los fines iniciales del tratamiento[157].

- Cifrado: Su uso corresponde a la obligación del responsable del tratamiento sobre la adopción de medidas para proteger a los datos del tratamiento ilícito, a través de su incorporación se impide el pirateo de la información[158].

- Anuladores de cookies: Estas herramientas bloquean las cookies introducidas por terceros en los ordenadores, que en alguno caso, emiten instrucciones o recopilan información sin que el usuario tenga conocimiento de ello[159]. Su incorporación responde al principio de licitud del tratamiento.

---

[154]Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales, *op. cit*., p 11.
[155] *Ibidem,* p. 7.
[156] *Ibidem,* p. 56.
[157] Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET), p.4.
[158] *Idem.*
[159] *Idem.*

- Plataforma de Preferencias de Privacidad, también conocida como P3P: permite que los usuarios de plataformas digitales comparen las políticas de privacidad en relación con la información que desean proporcionar.[160] Su incorporación fomenta que las personas tengan un mayor conocimiento sobre el tratamiento de sus datos y las finalidades con las que se realiza.

Javier Puyol sugiere que una vez que se haya separado al dato del titular y eliminada la posibilidad de identificar a una persona, los datos derivados de esta separación, ya no están sujetos la normativa vigente de protección de datos personales[161]. Entre las principales técnicas se hallan la disociación de los datos, la anonimización y la encriptación. Estas técnicas requieren de un procesamiento a partir de herramientas informáticas con la expectativa de que una vez hecha, no sea posible volver a unir el dato con el titular del mismo.[162] Personalmente, considero que la legislación continúa siendo aplicable, pues de conformidad con el numeral 3 de la LPDPPP, los datos personales no sólo son aquellos que hacen identificable a una persona, sino también a aquellos que pertenezcan a personas.

3.4 Certificación internacional.

La certificación de empresas privadas mediante estándares internacionales, plantea no sólo un reconocimiento a los entes que cumplan los lineamientos sino también, crea una red de alternativas seguras a la hora de elegir empresas proveedoras de servicios digitales, lo que a su vez otorga seguridad para el desempeño de la analítica de datos. Una vez que los actores que intervienen en la gestión y tratamiento de datos de forma conjunta como interconectada aún de forma internacional, cumplan con estándares internacionales, tendremos una certeza de estar más cerca de brindar una protección más amplia para las personas.

---

[160] *Idem.*
[161] Puyol Moreno, Javier, “Una aproximación a big data”, Revista de Derecho UNED, s.l.i., núm. 14, 014, p. 304.
[162] *Ibidem*, p. 306.

A continuación se enuncian las normas no vinculantes que el INAI recomienda[163] al sector privado en materia de protección de datos personales que son relevantes como modelos de certificación de estándares de protección de datos:

- ISO/IEC 27001[164]
- ISO / IEC 27018 [165]
- ISO/IEC 27002[166]
- ISO/IEC 27005[167]
- ISO/IEC 27006[168]
- ISO/IEC TR 27008[169]
- ISO/IEC 29100[170]
- ISO/IEC 20000-1[171]

[163] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *Documentos de Interés. INAI,* disponible en *http://inicio.ifai.org.mx/SitePages/Documentos-de-Interes.aspx?a=m3* (última fecha de consulta el 17 de octubre de 2019).
[164] Norma ISO/IEC 27001, disponible en *https://www.normas-iso.com/iso-27001/* (última fecha de consulta el 20 de octubre de 2019).
[165] Norma ISO / IEC 27018 2014, disponible en *https://www.normas-iso.com/iso-iec-27018-2014-requisitos-para-la-proteccion-de-la-informacion-de-identificacion-personal/* (última fecha de consulta el 20 de octubre de 2019).
[166] Norma ISO/IEC 27002, disponible en *http://iso27000.es/iso27002.html* (última fecha de consulta el 20 de octubre de 2019).
[167] Norma ISO/IEC 27005, disponible en *https://www.iso.org/standard/75281.html* (última fecha de consulta el 20 de octubre de 2019).
[168] Norma ISO/IEC 27006, disponible en *http://inicio.ifai.org.mx/DocumentosdeInteres/4_4_ISO27006.pdf* (última fecha de consulta el 20 de octubre de 2019).
[169] Norma ISO/IEC TR 27008, disponible en *http://inicio.ifai.org.mx/DocumentosdeInteres/4_5_ISO27008.pdf* (última fecha de consulta el 20 de octubre de 2019).
[170] Norma ISO/IEC 29100, disponible en *https://www.normas-iso.com/iso-iec-29100-framework-sobre-protecccion-de-datos-de-informacion-personal/* (última fecha de consulta el 20 de octubre de 2019).
[171] Norma ISO/IEC 20000-1, disponible en *https://www.normas-iso.com/iso-20000/* (última fecha de consulta el 20 de octubre de 2019).

- ISO 22301[172]
- ISO 31000[173]
- ISO GUIDE 72[174]
- ISO GUIDE 73[175]
- ISO 9000[176]

Además, de las normas ISO, El INAI enuncia otros estándares internacionales en materia de protección de datos, entre los que se enuncian los siguientes:

- BS 10012:2009[177]
- NIST SP 800-14
- OECD Guidelines
- GAPP
- COBIT v4.1
- COBIT 5
- PCI DSS v2

[172] Norma ISO 22301, disponible en *http://inicio.ifai.org.mx/DocumentosdeInteres/4_8_ISO22301.pdf* (última fecha de consulta el 20 de octubre de 2019).
[173] Norma ISO 31000, disponible en *http://inicio.ifai.org.mx/DocumentosdeInteres/4_9_ISO31000.pdf* (última fecha de consulta el 20 de octubre de 2019).
[174] Norma ISO GUIDE 72, disponible en *http://inicio.ifai.org.mx/DocumentosdeInteres/4_10_ISOGUIDE72.pdf* (última fecha de consulta el 20 de octubre de 2019).
[175] Norma ISO GUIDE 73, disponible en *http://inicio.ifai.org.mx/DocumentosdeInteres/4_11_ISOGUIDE73.pdf* (última fecha de consulta el el 20 de octubre de 2019).
[176] Norma ISO 9000, disponible en *http://inicio.ifai.org.mx/DocumentosdeInteres/4_12_ISO9000.pdf* (última fecha de consulta el 20 de octubre de 2019).
[177] Norma BS 10012:2009, disponible en *http://inicio.ifai.org.mx/DocumentosdeInteres/4_13_BS10012.pdf* (última fecha de consulta el 20 de octubre de 2019).

- HIPAASOx
- ITIL v3
- OWASP v2
- CCM v3 referente a
- Metodología de Análisis de Riesgo BAA
- Metodología de Análisis de Riesgo BAA

Conclusiones

Conclusiones.

La incorporación de tecnologías a numerosos aspectos de la vida ha fomentado la generación de cambios en la comprensión del mundo, en las relaciones comerciales, en las dinámicas sociales, económicas y por supuesto, en el derecho. Algunas de estas transformaciones, parten de una dualidad compatible entre el mundo digital y mundo físico. No obstante el ciberespacio hace gala de un enorme potencial para conectar a un gran número de personas, influir en ellas y analizar su información. A través de este, se ha gestado toda una nueva economía basada en los datos.

La voracidad con la que se desenvuelve la economía de los datos y las múltiples oportunidades para aprovechar la información obtenida a través de la analítica, fomenta que se desarrolle y alcance nuevos aspectos técnicos y comerciales para su explotación. Lo anterior genera posibilidades inmensas, tanto en oportunidades para atender necesidades de las personas, como ventajas competitivas entre empresas tecnológicas. Lo anterior ha derivado en diferentes ventajas tanto para los usuarios como para las empresas que trabajan con analítica de datos, pero también trae aparejado un mayor riesgo para la privacidad de las personas cuyos datos son tratados a través de las TIC.

La competencia entre los agentes tecnológicos, ha puesto y sigue poniendo en riesgo la protección de aspectos íntimos de las personas cuyos datos son recopilados, almacenados o procesados a través de tecnologías informáticas. Si bien, las normas jurídicas se han desenvuelto como la principal opción para la solución para los problemas sociales de un momento histórico en particular, su eficacia no radica en su mera existencia.

En el capítulo dos, se hizo un breve análisis de los principales instrumentos jurídicos para la regulación del tratamiento de los datos y la protección de la privacidad. Si bien, podemos observar que el marco jurídico nacional e internacional es sólido respecto a la protección contemplada en tales normas, la existencia de legislaciones, no garantiza el respeto de los derechos que se vislumbran en ellas.

Lo anterior se resume en la premisa de Hume, sobre la “imposibilidad de la deducción de juicios cuya cópula es un *debe* a partir de premisas cuya cópula es un *es*”.

Tal premisa es observable no sólo en el derecho informático, sino también, en todas las normas jurídicas en general y resulta en el reconocimiento de la limitación de la norma jurídica para surtir efectos directos sobre el mundo de los hechos. Aunado a lo anterior, el ejercicio de derechos en el ciberespacio se enfrenta también ante la dificultad de trasladar la fuerza del Estado al ciberespacio para actuar sobre lo que se considera legal o ilegal en el internet.

En este sentido, el ejercicio de derechos como la privacidad y la protección de los datos personales puede verse restringido y a merced de múltiples factores como la influencia de las empresas y operadores privados que fomentan y regulan muchas de las interacciones en el mundo digital. A su vez, la velocidad con la que suceden los actos y hechos en el ciberespacio supera en muchos casos a las herramientas con las que la autoridad cuenta para poner en marcha la maquinaria estatal.

Lo anterior, nos lleva a considerar nuevas estrategias para la protección de los datos personales con atención a dos aspectos primordiales: el humano y el tecnológico. Este último, a través de un enfoque de protección de los datos personales a través de tecnologías que contemplen medidas como la incorporación de sistemas PET y otros similares destinados a proteger el derecho a la intimidad a través de la reducción del uso de los datos personales, evitando el tratamiento innecesario, sin menoscabo de la funcionalidad del sistema de información.

Esto supone la incorporación de tecnologías como la disociación de los datos personales, la anonimización y la encriptación desde el diseño en las herramientas de procesamiento automatizado de datos. A su vez, es menester brindar un seguimiento de las buenas prácticas y las certificaciones en las empresas privadas con la incorporación de una constante capacitación y sensibilización del capital humano de las empresas. Esto es indispensable para fomentar la consciencia sobre

la responsabilidad jurídica y social que los diseñadores y administradores de los sistemas informáticos albergan en sus manos para la protección de los datos personales.

Lograr la salvaguarda de los datos requiere de una colaboración conjunta y de la incorporación de herramientas de procesamiento automatizado de datos. De esta manera se brindará una protección a otros derechos que se desarrollan en conjunto como los son el derecho de privacidad y el derecho a la dignidad humana como la seguridad de la información, la transparencia y la no discriminación.

Derivado de lo anterior, se requiere fomentar la incorporación de una perspectiva social y ética en la formación de especialistas destinados a elaborar o trabajar con herramientas informáticas y la puesta en marcha de campañas de difusión sobre los mecanismos de cumplimiento y salvaguarda de derechos, por parte de los responsables de su tratamiento con el fin de incorporar aspectos como la privacidad por diseño en los procesos y programas que incluyan el tratamiento de datos personales.

El factor humano es indispensable para la salvaguarda de los derechos en el ciberespacio. Es necesario concientizar también a los titulares de los datos para dotarlos de herramientas y conocimiento suficiente para tomar acciones destinadas a proteger su información y exigir lo mismo ante los responsables del tratamiento. Lo anterior conlleva el fomento y seguimiento de políticas públicas destinadas a la población en general con el fin de promover la educación de las personas en relación con el conocimiento del ejercicio de sus derechos. Esto es relevante para fomentar una cultura de la prevención y de desarrollo de habilidades para el uso responsable de las TIC en la que participen, el Estado, la iniciativa privada, la academia y la sociedad.

Bibliografía

Bibliografía.

Libros.

ACUÑA LLAMAS, Francisco Javier, “La protección de los datos personales y notas sobre los desafíos de internet”, en Recio Gayo, Miguel, (comp.), *La constitución en la sociedad y economía digitales: Temas selectos de derecho digital mexicano*, México, 2016

ADAME GODDARD, Jorge, *Diccionario Jurídico Mexicano*, Universidad Nacional Autónoma de México, México, 1983, t. II

MARR, Bernard, *Data Strategy: Cómo beneficiarse de un mundo de Big Data, Analytics e internet de las cosas*, Trad. Ramia Inés y Jimenez Alicia, s.l.i., Editorial Teell, 2018

DÍAZ, Vanesa, “El ejercicio de los Derechos ARCO ante el flujo trasfronterizo de información biométrica”, en Téllez Carvajal, Evelyn (comp.), *Derecho y TIC. Vertientes actuales*, México, Instituto de Investigaciones Jurídicas de la UNAM, 2016

LEFRANC WEEGAN, Federico César, *Terra Incógnita Bases para una política criminal pro persona en la sociedad digital*, México, Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación, 2015

National Science and Technology Council, *Privacy & Biometrics. Building a conceptual foundation.* s.l.i., Createspace Independent Publishing Platform, 2006

PACKARD, Ashley, *Digital media law*, 2a. ed., Wiley-Blackwell, s.l.i., 2013

PÉREZ MARQUÉS, María, *Big Data, Técnicas, herramientas y aplicaciones*, México, Editorial Alfaomega Grupo Editor S.A. de C.V., 2015

PIÑAR MAÑAS, José Luis, (Coord.) *La protección de datos personales en México*, México, Tirant lo Blanch Monografías, 2013

PULIDO JIMÉNEZ, Miguel, *Convergencias y divergencias: Acceso a la Información y la tutela de los datos personales*, *Retos de la protección de dato personales en el sector público*, México, Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, 2011, disponible en *http://www.infodf.org.mx/comsoc/campana/2012/LIbrozdatosPweb.pdf* (última fecha de consulta el 12 de septiembre de 2019)

VELANDIA Carolina y Prada, Fredy Alexander, "La protección de los datos digitales. Una lectura de la tensión del habeas data en el contexto del cambio de las relaciones sociales que supone internet" en Téllez Carvajal, Evelyn, (comp.), *Derecho y TIC. Vertientes actuales*, México, Instituto de Investigaciones Jurídicas de la UNAM, 2016

VILLANUEVA Ernesto y DÍAZ Vanesa, *Derecho de las nuevas tecnologías (en el siglo XX derecho informático)*, México, Oxford University Press, 2015

Revistas.

BRAGANZA Ashley, *et al*. "Resource management in big data initiatives: Processes and dynamic capabilities", *Journal of Business Research*, s.l.i., Volumen 70, 2017, enero de 2017, disponible en *https://reader.elsevier.com/reader/sd/pii/S0148296316304933?token=F96B045156186A1BB50B0C9825BC60F4EC92B4E3B356481D68104138D7B5F61A99A980D0B238AE47DB00CD45D2670D82* (última fecha de consulta el 29 de septiembre de 2019)

ESCALANTE GONZALVO Fernando, "El derecho a la privacidad, México", *Cuadernos de Transparencia 02,* Instituto Federal de Acceso a la Información Pública, México, 2004, disponible en *https://biblio.juridicas.unam.mx/bjv/detalle-libro/1798-cuadernos-de-*

transparencia-02-el-derecho-a-la-privacidad (última fecha de consulta el 11 de agosto de 2019)

EREVELLES Sunil, *et al*., "Big data consumer analytics and the transformation of marketing", *Journal of Business Research*, s.l.i., 2016, num. 69, consultado el 13 de septiembre de 2019, disponible en *https://www.samiagamoura.com/_media/1.-paper-big-data-marketing.pdf* (última fecha de consulta el 13 de septiembre de 2019)

GANDOMI Amir y Haider, Murtaza, "Beyond the hype: Big data concepts, methods, andanalytics", *Journal of Business Research*, s.l.i. Volumen 35, 2015, disponible en *https://www.sciencedirect.com/science/article/pii/S0268401214001066?via%3Dihub#bib0115* (última fecha de consulta el 21 de agosto de 2019)

GARZÓN VALDEZ, Ernesto, "Lo íntimo, lo privado y lo público", *Cuadernos de transparencia*, 5ª. ed., México, Instituto Federal de Acceso a la Información Pública, 2008

GONZALEZ GUERRERO, Laura Daniela, "Control de nuestros datos personales en la era del *big data:* el caso del rastreo web de terceros", *Estudios. Socio-Jurídicos*, Bogotá, vol. 21, 2019, disponible en *http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0124-05792019000100209&lang=es* (última fecha de consulta el 11 de octubre de 2019)

GONZÁLEZ RODRÍGUEZ, Arnaíz Graciano, "El imperativo tecnológico una alternativa desde el humanismo", *Cuadernos de bioética*, España, Vol. 15, Num. 53, 2004, disponible en *http://aebioetica.org/revistas/2004/15/1/53/37.pdf* (última fecha de consulta el 9 de octubre de 2019)

HOEPMAN, Jaap-Henk*, "*Privacy Design Strategies", Cuppens-Boulahia N, *et. al*., *ICT Systems Security and Privacy Protection*., vol 428., Springer, Berlin,

Heidelberg, 2014, p. 5, disponible en *https://www.cs.ru.nl/~jhh/publications/pdp.pdf* (última fecha de consulta 17 de noviembre de 2019)

LANEY, Doug, Aplication Delivery Strategies, "3D Management: Controlling Data Volume, Velocity, an Variety", *ApplicationDelivery Strategies*, META Group Inc., File 949, 2001, disponible en *http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf* (última fecha de consulta el 3 de octubre de 2019)

Loup Ventures, *Annual Smart Speaker IQ Test*, disponible en *https://loupventures.com/annual-smart-speaker-iq-test/* (última fecha de consulta el 7 de octubre de 2019)

MARSHALL MCLUHAN, Herbert, "At the moment of Sputnik the planet became a global teather in wich there are no spectators bur only actors" *Journal of Communication*, s.l.i., vol. 24, num. 1, invierno de 1974, disponible en *https://academic.oup.com/joc/article/24/1/48/4553567* (última fecha de consulta el 8 de septiembre de 2019)

MENDOZA ENRÍQUEZ Olivia Andrea, "Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento", *ius Revista del Instituto de Ciencias Jurídicas de Puebla*, México. vol. 12, num. 41., enero-junio de 2018

ORNELAS NUÑEZ, Lina y Piñar Mañas, "Los principios de la protección de datos personales", en Ornelas Nuñez, Lina y Piñar Mañas, *La protección de datos personales en México*, México, México, Tirant lo Blanch Monografías, 2013, disponible en *https://www.tirant.com/mex/libro/la-proteccion-de-datos-personales-en-mexico-9788490336793* (última fecha de consulta el 30 de mayo de 2019)

OSORIO CARLOS, "La participación pública en sistemas tecnológicos. Lecciones para la educación CTS", *Revista iberoamericana de ciencia, tecnología y*

sociedad, Buenos Aires, vol. 2, num. 6, 2005, disponible en *http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-36282012000200003&lang=es* (última fecha de consulta el 8 de mayo de 2019)

PUYOL MORENO, Javier, "Una aproximación a big data*"*, *Revista de Derecho UNED*, s.l.i., núm. 14, RDUNED, 2014

SKEEM Jennifer y LOWENKAMP Christopher T, "Risk, Race, & Recidivism: Predictive Bias and Disparate Impact", *Criminology and Public Policy, Forthcoming, University of Chicago Law & Economics Olin Working Paper, s.l.i.,* Columbia University, 2010, *No. 535*, p. 11, Disponible en *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2687339* (última fecha de consulta 16 de octubre de 2019)

WARREN, Samuel D. y BRANDEIS, Louis D., "The Right to Privacy", *Harvard Law Review*, s.l.i, Vol. 4, Num. 5. Diciembre de 1890, disponible en *https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf* (última fecha de consulta el 5 de agosto de 2019)

WIDOW LIRA, Felipe, "La ley de Hume en Hume: la discusión de la interpretación analítica de Treatise III, 1, i," *Anales del Seminario de Historia de la Filosofía,* vol. 32, num. 2, 2015, disponible en *https://revistas.ucm.es/index.php/ASHF/article/view/49971* (última fecha de consulta el 19 de octubre de 2019)

Comunicados y documentos electrónicos.

Agencia Española de Protección de Datos, *Guía de Privacidad desde el Diseño*, *s.l.i, 2019,* disponible en *https://www.aepd.es/media/guias/guia-privacidad-desde-diseno.pdf* (última fecha de consulta el 1 de agosto de 2019)

Agencia Española de Protección de datos, *Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD, de la Agencia Española de Protección de datos*, disponible en

https://d3t4nwcgmfrp9x.cloudfront.net/upload/AnalisisDeRiesgosRGPD.pdf (última fecha de consulta el 8 de agosto de 2019)

ANGWIN Julia*, et al., Machine Bias There's software used across the country to predict future criminals. And it's biased against blacks,* ProPublica, disponible en *https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing* (última fecha de consulta el 3 de septiembre de 2019)

ASKELL Amanda, *The Role of Cooperation in Responsible AI Development*, disponible en *https://arxiv.org/pdf/1907.04534.pdf* (última fecha de consulta octubre de 2019)

Asociación Mexicana de Internet, *Estudio de Protección de Datos Personales entre Usuarios y Empresas realizado por la Asociación Mexicana de Internet [AMIPCI] sobre una base de 734 usuarios de plataformas digitales y 187 empresas evaluadas*, disponible en *https://www.asociaciondeinternet.mx/es/component/remository/func-startdown/19/lang,es-es/?Itemid=* (última fecha de consulta el 11 de junio de 2019)

BRADSHAW Samantha y HOWARD Philip N., *The Global Disinformation Order 2019 Global Inventory of Organised Social Media Manipulation*, Oxford Internet Institute, University of Oxford, 2019, disponible en *https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf* (última fecha de consulta el 29 de septiembre de 2019)

BRUNDAGE Miles*, et al. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, Future of Humanity, Institute University of Oxford, Centre for the Study of Existential Risk, University of Cambridge, Center for a New American Security, Electronic Frontier Foundation, OpenAI, disponible en *https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf* (última fecha de consulta octubre de 2018)

Comisión Presidencial Coordinadora de la política del ejecutivo en materia de Derechos Humanos-COPREDEH, *Pacto Internacional de los Derechos Civiles y Políticos, versión comentada*, Guatemala, 2011, disponible en *http://www.aprodeh.org.pe/documentos/marco-normativo/legal/Pacto-Internacional- de-Derechos-Civiles-y-Politicos.pdf* (última fecha de consulta el 23 de agosto de 2019)

Instituto Nacional de Estadística y Geografía*, Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares*, 2018, disponible en *https://www.inegi.org.mx/programas/dutih/2018/default.html#* (última fecha de consulta el 5 de octubre de 2019)

Instituto Nacional de Geografía y Estadística, *Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales (ENAID),* disponible en *https://www.inegi.org.mx/programas/enaid/2016/* (última fecha de consulta el 17 de marzo de 2019)

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *Documentos de Interés. INAI,* disponible en *http://inicio.ifai.org.mx/SitePages/Documentos-de-Interes.aspx?a=m3* (última fecha de consulta el 17 de octubre de 2019)

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *El ABC del Aviso de Privacidad*, disponible en *http://abcavisosprivacidad.ifai.org.mx/* (última fecha de consulta el 17 de octubre de 2019)

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *Evaluador de Vulneraciones*, disponible en *http://inicio.ifai.org.mx/SitePages/Evaluador-Vulneraciones.aspx* (última fecha de consulta el 15 de octubre de 2019)

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales , *Guía para implementar un Sistema de Gestión de Seguridad de*

Datos Personales Junio 2015, disponible en *http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf* (última fecha de consulta el 9 de agosto de 2019)

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *Guía para el tratamiento de datos biométricos*, México, Edición Marzo 2018, disponible en *http://inicio.ifai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.pdf* (última fecha de consulta el 27 de julio de 2019)

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*, Guía para prevenir el robo de identidad*, disponible en *http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Prevenir_RI.pdf* (última fecha de consulta el 7 de agosto de 2019)

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *Sistema Generador de Avisos de Privacidad*, disponible en *https://generador-avisos-privacidad.inai.org.mx/* (última fecha de consulta el 17 de octubre de 2019)

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *Vulnerómetro*, disponible en *https://micrositios.inai.org.mx/vulnerometro/index.php* (última fecha de consulta el 7 de agosto de 2019)

Norma BS 10012:2009, disponible en *http://inicio.ifai.org.mx/DocumentosdeInteres/4_13_BS10012.pdf* (última fecha de consulta el 20 de octubre de 2019)

Norma ISO/IEC 20000-1, disponible en *https://www.normas-iso.com/iso-20000/* (última fecha de consulta el 20 de octubre de 2019)

Norma ISO 22301, disponible en *http://inicio.ifai.org.mx/DocumentosdeInteres/4_8_ISO22301.pdf* (última fecha de consulta el 20 de octubre de 2019)

Norma ISO/IEC 27001, disponible en *https://www.normas-iso.com/iso-27001/* (última fecha de consulta el 20 de octubre de 2019)

Norma ISO/IEC 27002, disponible en *http://iso27000.es/iso27002.html* (última fecha de consulta el 20 de octubre de 2019)

Norma ISO/IEC 27005, disponible en *https://www.iso.org/standard/75281.html* (última fecha de consulta el 20 de octubre de 2019)

Norma ISO/IEC 27006, disponible en *http://inicio.ifai.org.mx/DocumentosdeInteres/4_4_ISO27006.pdf* (última fecha de consulta el 20 de octubre de 2019)

Norma ISO/IEC TR 27008, disponible en *http://inicio.ifai.org.mx/DocumentosdeInteres/4_5_ISO27008.pdf* (última fecha de consulta el 20 de octubre de 2019)

Norma ISO / IEC 27018 2014, disponible en *https://www.normas-iso.com/iso-iec-27018-2014-requisitos-para-la-proteccion-de-la-informacion-de-identificacion-personal/* (última fecha de consulta el 20 de octubre de 2019)

Norma ISO/IEC 29100, disponible en *https://www.normas-iso.com/iso-iec-29100-framework-sobre-protecccion-de-datos-de-informacion-personal/* (última fecha de consulta el 20 de octubre de 2019)

Norma ISO 31000, disponible en *http://inicio.ifai.org.mx/DocumentosdeInteres/4_9_ISO31000.pdf* (última fecha de consulta el 20 de octubre de 2019)

Norma ISO 9000, disponible en *http://inicio.ifai.org.mx/DocumentosdeInteres/4_12_ISO9000.pdf* (última fecha de consulta el 20 de octubre de 2019)

Norma ISO GUIDE 72, disponible en *http://inicio.ifai.org.mx/DocumentosdeInteres/4_10_ISOGUIDE72.pdf* (última fecha de consulta el 20 de octubre de 2019)

Norma ISO GUIDE 73, disponible en *http://inicio.ifai.org.mx/DocumentosdeInteres/4_11_ISOGUIDE73.pdf* (última fecha de consulta el el 20 de octubre de 2019)

Northpointe, *Practitioners guide to COMPAS core*, 2015, disponible en *https://www.documentcloud.org/documents/2840784-Practitioner-s-Guide-to-COMPAS-Core.html#document/p30/a296482* (última fecha de consulta el 14 de octubre de 2019)

Organización de las Naciones Unidas, *Informe sobre la economía digital 2019, Creación y captura de valor: repercusiones para los países en desarrollo*, United Nations Publications, Nueva York, Ginebra, 2019, disponible en *http://www.onu.org.mx/wp-content/uploads/2019/09/unctad_esp.pdf* (última fecha de consulta el 11 de agosto de 2019)

Organización para la Cooperación y el Desarrollo Económicos, *Recommendation of the Council on Artificial Intelligence*, disponible en *https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449* (última fecha de consulta el 11 de septiembre de 2019)

Unión Internacional de Telecomunicaciones, *Informe sobre Medición de la Sociedad de la Información*, Resumen analítico 2018, ITU Publicaciones, 2018, disponible en *https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR2018-ES-PDF-S.pdf* (última fecha de consulta el 8 de septiembre de 2019)

Notas periodísticas y sitios electrónicos.

ALBA Davey y SATARIANO Adam, “At Least 70 Countries Have Had Disinformation Campaigns, Study Finds.”, *The New York Times*, publicado el 26 de septiembre de 2019, Section B, Disponible en

https://www.nytimes.com/2019/09/26/technology/government-disinformation-cyber-troops.html (última fecha de consulta el 27 de octubre de 2019)

Domo, *Data Never Sleeps 7.0*, disponible en *https://www.domo.com/learn/data-never-sleeps-7* (última fecha de consulta el 1 de octubre de 2019)

Gartner, *Gartner Glossary,* disponible en *https://www.gartner.com/it-glossary/big-data/* (última fecha de consulta el 7 de septiembre de 2019)

Google, *How Google's featured snippets work*, disponible en *https://support.google.com/websearch/answer/9351707 (última fecha de* consulta el 8 de octubre de 2019)

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *¿Cómo ejercer el derecho a la protección de datos personales?,* disponible en *http://inicio.ifai.org.mx/SitePages/Como-ejercer-tu-derecho-a-proteccion-de-datos.aspx?a=m1* (última fecha de consulta el 25 de julio de 2019)

LARSON Jeff*, et al.*, *How We Analyzed the COMPAS Recidivism Algorithm*, Propublica, disponible en *https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm* (última fecha de consulta el 3 de septiembre de 2019)

Las Iniciativas de EE UU En Materia de Ia y el Futuro de los Gobiernos, disponible en *https://www.ma-no.org/es/las-iniciativas-de-ee-uu-en-materia-de-ia-y-el-futuro-de-los-gobiernos* (última fecha de consulta el 13 de octubre)

Loup Ventures, *Annual Smart Speaker IQ Test*, disponible en *https://loupventures.com/annual-smart-speaker-iq-test/* (última fecha de consulta el 7 de octubre de 2019)

Moral Machine , *About Moral Machine*, disponible en http://moralmachine.mit.edu/ (última fecha de consulta el 6 de septiembre de 2019)

Organización de las Naciones Unidas, *¿Qué son los derechos humanos?,* disponible en *https://www.hchr.org.mx/index.php?option=com_content&view=article&id=448&Itemid=249* (última fecha de consulta el 23 de agosto de 2019)

Organización para la Cooperación y el Desarrollo Económicos, *What are the OECD Principles on AI?*, disponible en *http://www.oecd.org/going-digital/ai/principles/* (última fecha de consulta el 15 de octubre de 2019)

Real Academia Española, Diccionario Español Jurídico, disponible en *https://dej.rae.es/lema/big-data* (última fecha de consulta el 25 de septiembre de 2019)

SnapPay, *Biometrics SnapPay Merchants Can Now Accept Facial Recognition Payments*, disponible en *https://www.pymnts.com/news/biometrics/2019/snappay-merchants-can-accept-facial-recognition-payments/* (última fecha de consulta el 17 de octubre)

SnapPay, *SnapPay,* disponible en *https://www.snappay.ca/* (última fecha de consulta el 17 de octubre de 2019)

Sullivan, Danny, *How we keep Search relevant and useful*, disponible en *https://www.blog.google/products/search/how-we-keep-google-search-relevant-and-useful/* (última fecha de consulta el 29 de septiembre)

¿Qué es la inteligencia artificial?, disponible en *https://definicion.de/inteligencia-artificial/* (última fecha de consulta el 3 de septiembre de 2019)

SAP, *¿Qué es la inteligencia artificial?*, disponible en *https://www.salesforce.com/mx/blog/2017/6/Que-es-la-inteligencia-artificial.html* (última fecha de consulta el 5 de septiembre de 2019)

Normativa nacional.

Constitución Política de los Estados Unidos Mexicanos

Código Civil Federal

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

Ley Federal de Protección de Datos Personales en Posesión de los Particulares

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental del 11 de junio de 2002 (derogada)

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

Tesis I.10o. A.6 CS, Semanario Judicial de la Federación y su Gaceta, Décima Época, t. III, Septiembre de 2019, p. 2200

Tesis I.10o. A.5 CS, Semanario Judicial de la Federación y su Gaceta, Décima Época, t. III, Septiembre de 2019, p. 2199

Normativa internacional.

Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET), realizado en Bruselas, 2007

Convención americana sobre derechos humanos o Pacto de San José de Costa Rica

Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal

Declaración Universal de Derechos Humanos

Declaración Americana de los Derechos y Deberes del Hombre

Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales

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

Ley 25.326 de Protección de Datos Personales de Argentina

Marco de Privacidad del foro de Cooperación Económica Asia-Pacífico [APEC], también conocido como el Sistema de Reglas de Privacidad Transfronteriza (*Cross-Border Privacy Rules CBPRs*)

Pacto internacional de derechos civiles y políticos

Recomendación del Consejo de Inteligencia Artificial de la Organización para la Cooperación y el Desarrollo Económicos

Recomendaciones en materia de seguridad de datos personales, publicadas en el Diario Oficial de la Federación el 30 de octubre de 2013

Reglamento (UE) 2018/1725 del Parlamento Europeo y del consejo de 23 de octubre de 2018 Relativo a la Protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.o 45/2001 y la Decisión n.o 1247/2002/CE

Anexos

Siglas y abreviaturas

APEC: Marco de Privacidad del foro de Cooperación Económica Asia-Pacífico

ENAID: Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales

IA: Inteligencia Artificial

IFAI: Instituto Federal de Acceso a la Información

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

INEGI: Instituto Nacional de Geografía y Estadística

ISO: International Organization for Standardization, de conformidad con su traducción es la Organización Internacional de Normalización o Estandarización

LFPDPPP: Ley Federal de Protección de Datos Personales en Posesión de los Particulares

LFTAIPG: Ley Federal de Transparencia y Acceso a la Información Pública

LGPDPPSO: Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados

OCDE: Organización para la Cooperación y el Desarrollo Económicos

ONU: Organización de las Naciones Unidas

P3P: Plataforma de Preferencias de Privacidad

PET: Private enhance technologies o Tecnologías de Mejora de Privacidad por su traducción al español

RGPD: Reglamento General de Protección de Datos

TIC: Tecnologías de Información y Comunicación

TJUE: Tribunal de Justicia de la Unión Europea

Glosario

Big Data: Gran cantidad de información en formato digital que para su análisis y procesamiento requiere de herramientas tecnológicas.

Bot: Se conoce como bot a un programa informático que realiza tareas repetitivas a través de internet.

Blockchain: La traducción al español es cadena de bloques y hace referencia a una estructura de datos que se agrupa en bloques, cuya modificación no puede ser efectuada de forma independiente sino en todos los bloques de la cadena. Aunado a lo anterior, la incorporación de tecnologías encriptación provee un mayor nivel de seguridad a la información almacenada.

Código QR: Las siglas QR corresponden a Quick Response en referencia a la velocidad de lectura del código. Éste se compone de una serie de recuadros con una distribución única, lo cual permite alojar información que puede ser descifrada a través de un lector especializado para ello.

Cookies: En la informática, las cookies hacen referencia a información que un sitio web aloja en un navegador para recopilar información del comportamiento del usuario.

Cloud computing: También conocido como cómputo en la nube por su traducción al español, es una tendencia tecnológica que supone el traslado de procesos que usualmente suceden en los ordenadores de los usuarios, a la nube. Se entiende por nube a un sistema de servidores conectados a los cuales se puede acceder a través de redes como el internet. El cloud computing supone una nueva forma de acceder a servicios, almacenamiento, procesos, aplicaciones y software de manera remota con una mayor rapidez y menores costos para los usuarios.

Criptomonedas: También son conocidas como criptodivisas o criptoactivos y corresponden a un tipo de divisa o moneda digital que incorpora la criptografía como medio para blindar a las transacciones y activos a través de medios digitales.

Cyborg: También conocido como ciborg, es un acrónimo de cibernético y organismo. Se entiende como cyborg a un ser que se compone de elementos orgánicos y cibernéticos. Para efectos de la presente investigación, se hace referencia a programas cibernéticos automatizados combinados con la supervisión e intervención humana.

Data Broker: Terceros que cuentan con grandes datos o información y que son intermediarios entre la fuente de los datos y aquellos quienes pueden aprovecharlos con distintos fines como ventas, mercadotecnia, análisis de información, etc.

Geolocalización: Tecnología que permite hallar la ubicación geográfica de un dispositivo. La geolocalización es usada en diversos rubros, entre los que se encuentra su empleo en aplicaciones móviles de los teléfonos celulares, autotransportes, drones e incluso sobre seres vivos como medio para ubicar a ganado u otras especies animales.

Hardware: Componente físico de los dispositivos electrónicos.

Inteligencia Artificial: Se entiende como la emulación de la inteligencia huma a través de medios electrónicos. En algunos casos es interpretada como el procesamiento automatizado de datos. Para efectos de la presente investigación se hace referencia a la segunda pues se considera que actualmente no existe un procesamiento de información tan sofisticado que imite a la inteligencia humana.

Internet of things: Su acrónimo reconocido es IoT, la traducción al español es Internet de las cosas, corresponde a la comunicación existente entre distintos objetos a través de la internet.

PET: Sistema que con ayuda de herramientas tecnológicas disminuye el uso indebido de datos personales y protege la intimidad de las personas, a la vez que continúa siendo funcional como sistema de información.

Redes sociales: Son espacios virtuales que a través de la internet conectan en tiempo real a un gran número de personas para intercambiar información. En

muchos casos las redes sociales agrupan a personas con intereses similares o con un vínculo ya existente en el mundo físico.

Software: Es el conjunto de aplicaciones informáticas compuestas por algoritmos destinados a gestar una interoperación interna y en su caso comunicación los componentes físicos de los dispositivos. Ejemplo de lo anterior son el sistema operativo y las aplicaciones móviles.

Wearables: Dispositivos inteligentes que pueden ser vestidos por el usuario. Algunos ejemplos son anteojos, ropa o relojes inteligentes conectados al internet y que envían o reciben información del usuario y de la web.