Defensa de la privacidad digital: uso de datos biométricos en México

Defense of digital privacy: use of biometric data in Mexico

Rodolfo Guerrero Martínez[1]

Sumario: I. Introducción. II. Privacidad, Intimidad y su multidimensionalidad. III. Biometría y Sistemas Biométricos. IV. Privacidad Digital y su Defensa. V. Ciberseguridad y Biometría. VI. Comentarios y Análisis de Protección de datos personales en México. VII. Conclusión. VIII. Referencias bibliográficas.

Fecha de recepción: 15 de octubre de 2021
Fecha de aceptación: 23 de diciembre de 2021

La vida privada de un ciudadano debe ser recinto amurallado.
Príncipe Talleyrand

Resumen
A partir de la nueva realidad consecuencia de la pandemia por COVID-19 se detonó, exponencialmente, la aplicación y avance de las tecnologías de la información y de la comunicación en un desarrollo aproximado a diez años, se generaron diversos dilemas y problemas; uno de ellos por el déficit en legislación especial que tutele y garantice la protección de los derechos humanos y sus garantías, la privacidad en contextos virtuales y digitales, además de abrir el debate sobre la viabilidad de mecanismos, padrones y sistemas que almacenan datos biométricos de la población.

Abstract:
From the new reality product of the COVID-19 pandemic, exponentially detonated the application and development of information and communication technologies in an approximate development of ten years, thus generating several dilemmas and problems, one of them due to the deficit in particular legislation that protects and guarantees the protection of human rights and their guarantees, privacy in virtual and digital contexts, in addition to opening the debate on the viability of mechanisms, standards and systems that store biometric data of the population.

Palabras clave: Dilema. Tecnología. Biometría. Ciberseguridad. Privacidad.
Keywords: *Dilemma. Technology. Biometrics Cyber security. Privacy.*

1. Abogado por la Benemérita Universidad de Guadalajara, actualmente es estudiante del posgrado en derecho con orientación en materia Constitucional y administrativo por la misma casa de estudios. Es Socio Fundador y Representante Legal de la Sociedad Civil Coffee Law "Dr. Jorge Fernández Ruiz". Socio fundador de la Academia Mexicana de Derecho "Juan Velásquez" A.C. Miembro de la Junta Menor y encargado de la Comisión de Legaltech del Ilustre y Nacional Colegio de Abogados de México A.C. Capítulo Occidente. Vicepresidente de la Academia Mexicana de Derecho Informático, Capítulo Jalisco.

I. Introducción

Obligatoriamente, al desempeñar las causas de interés a raíz de la innovación tecnológica conduce a recordar los antecedentes, en particular, donde surge el origen de la privacidad por los trabajos desempeñados en Estados Unidos de Norteamérica en 1890 por Samuel D. Warren y Louis D. Brandeis, autores del artículo The right to privacy, que pronunció los cambios en las sociedades desde diferentes rubros, como el social, económico y político, donde se involucró el reconocimiento de los derechos de privacidad y protección a la información personal.

Al colocar el derecho a la protección de su vida privada, Warren y Brandeis establecían ir contra injerencias de los medios de información, lo cual tenía precedente en la regulación francesa en materia de prensa sin especificar de manera exacta el concepto de privacidad o the right to privacy; "derecho a ser dejado solo".

No obstante, existe un dilema sobre el reconocimiento armónico de privacidad debido a la falta de uniformidad en el uso de conceptos como privacy, vié privée y vida privada. Por ejemplo, en la versión en inglés de la Declaración Universal de los Derechos Humanos, en su artículo 12, menciona privacy de la siguiente manera: Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honor y reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques (1948). Mientras que en español se utiliza el término de vida privada. Se justifica el uso indistinto del mismo derecho en cada traducción, se omite dentro del documento qué debe entenderse en las expresiones del concepto.

La aprobación de 269 resoluciones resulta bastante interesante y oportuno que en el 45° periodo de sesiones de la Asamblea General de las Naciones Unidas, desarrolladas entre 1990 y 1991, destaque la Resolución 45/95, del 14 de diciembre de 1990, por la que se aprueban los "Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales".[2] Dichos valores son: licitud, lealtad, exactitud, finalidad, acceso, no discriminación y seguridad.

En el contexto de la sociedad de la información, donde se desarrolla el comercio digital, además del gobierno electrónico en donde se realiza el tratamiento de datos personales, es valioso recordar "las Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales",[3] adoptadas en 1980 tras varios años de trabajo desempeñado por la Organización para la Cooperación y el Desarrollo Económico (OCDE) para que los Estados adecuaran sus marcos jurídicos y establecer la garantía de protección de los derechos humanos, como el derecho a la privacidad.

2. Esta resolución tiene como finalidad aprobar un proyecto de principios en los que se trabajaba con anterioridad, prueba de ello son las resoluciones 1990/38 del Consejo Económico y Social, del 25 de mayo de 1990; 44/132, del 15 de diciembre de 1989 de la Asamblea General; 1989/78 del Consejo Económico y Social, del 24 de mayo de 1989, y 1989/43, de la otrora Comisión de Derechos Humanos, del 6 de marzo de 1989, todas bajo el mismo título de "Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales".
3. Las directrices plantearon los principios de limitación de recogida de datos personales; de calidad de los datos personales; de especificación del propósito de la recogida de datos personales; de limitación de uso de los datos personales; de limitación de uso de los datos personales; de la salvaguardia de la seguridad para proteger los datos personales; de transparencia en cuanto a evolución, prácticas y políticas relativas a datos personales, de participación individual y de responsabilidad sobre todo controlador de datos personales. Disponible en: www.oecd.org/sti/ieconomy/15590267.pdf

En este trabajo desarrollaré puntualmente los tópicos de privacidad, intimidad y su multidimensionalidad, también la biometría y los sistemas biométricos, para, finalmente, generar algunos comentarios sobre la reciente reforma a la ley federal de telecomunicaciones y radiodifusión.

II. Privacidad, intimidad y su multidimensionalidad

Realizaré el análisis terminológico de intimidad tanto de la lengua castellana como de la inglesa, la cual verifica la procedencia latina del concepto; su esencia semántica se distingue de la contenida en el vocablo privacy. Ambas voces son usadas como sinónimos erróneamente tanto en la tradición jurídica como en el lenguaje cotidiano. En sentido etimológico "íntimo" afirma Desantes Guanter (1972: 18), en proceder del latino intimus, que es una variación filológica de intumus, forma superlativa del verbo intus, dentro. "Íntimo" e "intimidad" refieren a aquello que está lo más dentro posible, a lo más reservado y lo más profundamente sentido por el ser humano.

Respecto a la privacidad, ninguna definición de *privacy* es posible, porque lo concerniente a la vida privada es, fundamentalmente, una cuestión de valores, intereses y poder (Westin, 1967). Es posible señalar que, en el campo de la vida privada, aparece gobernado "en parte no desdeñable por las modas y las costumbres de la sociedad de la que forma parte, sujetas a cambios considerables, especialmente en nuestro tiempo (urabayen, 1977)".

La privacidad tiene varias dimensiones: la física y la social, así como la psicológica y la informativa (los datos personales), por ello, para hablar de privacidad, no es suficiente que la persona tenga control sobre alguna de las cuatro dimensiones, sino sobre todas ellas. Por ello, la idea de control del individuo o de autodeterminación informativa es clave para conceptualizar la privacidad.

La privacidad tiene límites dictados por los casos en los que se ponga en riesgo el interés público. Estas limitaciones justifican que las leyes permitan la injerencia de las autoridades en la vida privada de la persona. Por ejemplo, se justifica la intervención autoritaria en el ámbito privado cuando se requieren los datos sobre las comunicaciones de una persona para realizar una investigación judicial o cuando los padres aprovechan la esfera protegida de la familia para violentar a los hijos o si una persona ocupa un importante cargo público y se necesita identificar si sus decisiones conllevan un conflicto de interés.

En este escenario resulta oportuno concluir de manera parcial con el razonamiento del distinción entre ambos conceptos (privacidad e intimidad), distinción que es solo una cuestión de grado dentro de esta especie (una relación de género-especie); indica que la intimidad pertenece al ámbito de la privacidad, todo lo íntimo es privado, en cambio, no toda la información privada es información íntima (Tornabene, 2014), además, contrario a lo mencionado por

la autora, los asuntos íntimos son privados, pero no todos los aspectos privados son íntimos, es decir, para ser mejor deberá omitirse la palabra "todo", pues no resultaría que todo lo íntimo es privado.

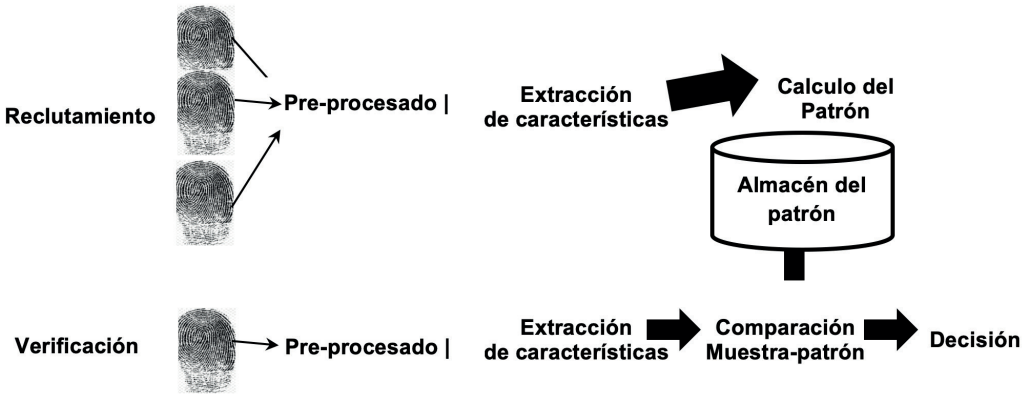
III. Biometría y sistemas biométricos

A pesar de que la biometría se considere como una ciencia futurista o parte de la ficción, sus principios básicos remontan hace miles de años, ello tras la comparación en la época de los faraones en el valle de Nilo, Egipto, donde esto se usaba para verificar a las personas que participaban en diferentes operaciones comerciales y judiciales (Umanick, 2014). Cabe resaltar que la biometría se implementaría en la cultura occidental hasta finales del siglo XIX, por ejemplo en Argentina hicieron desarrollo y aplicación de herramientas biométricas para el control del crimen, en buena parte atribuible a Juan Vucetich que creo el primer método de clasificación de huellas dactilares en 1891 (Anitua, 2005:19).

El concepto de biometría viene de las palabras bio (vida) y metría (medida), que significa que los equipos o sistemas identifican o miden alguna característica propia tanto de comportamiento como físico de una persona.

Lo anterior propone el uso de estas mediciones como metodologías de seguridad que permitan el reconocimiento de características físicas intransferibles de las personas para su identificación (Lervasi, 2005), mediante las técnicas biométricas de reconocimiento, las cuáles son muy diversas, debido a que todo elemento de una persona es utilizado para su identificación; no obstante, en el desarrollo de un sistema biométrico se produce un esquema totalmente independiente a la técnica efectuada, se puede ejemplificar en dos fases tanto la de reclutamiento como la de utilización diferenciada a 100 por cierto, como se observa en el siguiente diagrama.

Figura 1. Diagrama: Etapas en un Sistema de Identificación Biométrica



Fuente: Sanchez Reillo y otros, atl. 1999.

Existen dos tipos de mediciones biométricas: de comportamiento y la fisiológica. La fisiológica codifica las características físicas de los individuos, ya sea mediante la morfología que estudia el organismo y sus características, como huella digital, forma de la mano, patrón venoso, iris y retina, forma de la oreja o forma de la cara, o a través de la biología, que analiza el origen, evolución y propiedades de los organismos, como su ADN, sangre, saliva u orina, características normalmente de uso forense o médico. Estas mediciones generalmente son más confiables, pues permanecen estables a lo largo de la vida de la persona; sin embargo, solo tres son consideradas en verdad únicas y de precisión: retina, iris y huella digital (Woodward, 1997: 1,481).

III.1. Legislación

La ley de privacidad de datos de la Unión Europea (2018) define los datos biométricos como "categorías especiales de datos personales" y prohíbe su "procesamiento", lo que protege a las personas que su información se comparta con terceros sin su consentimiento. El 14 de septiembre de 2017, el proyecto de ley de protección de datos se publicó en el Reino Unido con la finalidad de modernizar la ley de protección de datos.

Es importante señalar que el Reglamento General de Protección de Datos Personales de la Unión Europea (GDPR) se aplicó en el Reino Unido a partir del 25 de mayo de 2018. El proyecto de ley de protección de datos solo se empleará cuando el GDPR deje a los Estados miembros la oportunidad de tomar medidas sobre cómo se administra en su país.

A partir de julio de 2017 en los Estados Unidos de Norteamérica es legal, en 47 estados, que el software identifique a una persona mediante imágenes tomadas sin consentimiento mientras está en público. Illinois y Texas no lo permiten para uso comercial. Washington fue el tercer estado en aprobar una ley de privacidad biométrica. Cubre cualquier entidad comercial que recolecta identificadores biométricos con fines comerciales.

III.2. Viabilidad y déficits de la biometría

Se dice que entre los beneficios que tiene esta tecnología sería la rapidez y lo amigable para los usuarios al ser necesario memorizar contraseñas, la autenticación de las características biológicas, la eliminación de fricción asociada con las medidas de seguridad tradicionales, además de los servidores biométricos que requieren de menos memoria en la base de datos.

Por otra parte, la gestión y la seguridad de identidad representan un problema, porque la información de identificación personal necesita tener acceso controlado para proteger contra robos de identidad, pues solo se requiere de un hacker para infiltrarse a cualquier base de datos y robar su identificación biométrica.

IV. Ciberseguridad y biometría

Cabe recordar que la identificación personal es la asociación entre la identidad y la persona, que se observa en forma de verificación o autentificación y reconocimiento (Jain, Bolle y Pankati, 1996). Es importante tenerlo presente para dimensionar la delicada situación ante la era digital y cómo se vuelve indispensable la práctica de la ciberseguridad, incluso como un derecho humano de última generación.

Es preciso destacar dos conceptos para la unificación y comprensión de escenarios entre la ciberseguridad y la biometría, el primero entendido como la "Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados" (ISACA, 2015).

En cuanto al segundo, que es la biometría, son aquellos métodos automáticos para el reconocimiento único de humanos, basados en rasgos físicos o conductuales intrínsecos a las personas. Asimismo, las características biométricas, como huellas dactilares, iris o retina oculares, voz, o incluso los latidos del corazón y las expresiones faciales, proporcionan beneficios en sistemas de identificación tanto en comodidad y facilidad de uso como en sus características inequívocas para cada persona.

El objeto de lo anterior es que se cuestione ¿de qué manera somos propensos a ser víctimas de una suplantación biométrica? Seguramente lo tradicional es el delito de suplantación de identidad previsto en México en el Código Penal Federal, pero ahora, ante la innovación y progreso tecnológico, esta amenaza resalta más.

Debido que los sistemas biométricos son usados para asegurar teléfonos o tabletas, son vulnerables a que se les muestre una fotografía del propietario y permitan el desbloqueo del dispositivo, ello representa un riesgo para cualquier empresa o dependencia gubernamental.

IV.1. Problemas de rasgos biométricos

Pese a que se desarrollen sistemas biométricos avanzados que supuestamente no pueden ser burlados no existe garantía que, pasado un tiempo, aún sean seguros, pues la tecnología avanza rápidamente, y recursos técnicos que hoy serían impensables para un posible atacante, posteriormente, pueden estar al alcance de cualquier persona. Precisamente comprender el valor de nuestros datos personales es fundamental, debido a que en el caso biométrico nuestros rasgos seguirán siendo los mismos y ya los habríamos perdido, al dejarlos bajo la protección de una sola parte o sistema.

Enfatizar en la definición concreta de dato personal por parte del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos

Personales es crucial, pues señala que el dato personal será todo aquello que nos permita identificarnos y nos haga identificables, en lo último, alude a los datos biométricos.

Los problemas son diversos (Rodríguez, 2013)

- Son únicos, permanentes e irrevocables.
- Públicos y de obtención es sencilla.
- Replicables con facilidad.
- No se pueden denegar.
- Pueden ser usurpados por medios fuera del control del propietario y - la información extraída de un rasgo biométrico deberá ser almacenada en algún tipo de base de datos, lo cual propicia no solo el robo físico, sino que compromete el lugar con ingeniera inversa o expone la seguridad de un servidor o base de datos.
- Los sistemas presentan un área de ataque más amplia. Los atentados podrán ser en áreas tan discrepantes como: la audiovisual, en la medicina, mecánica, química, electrónica e incluso en la física aplicada.

V. Privacidad digital y su defensa

Desde el uso masivo de las plataformas digitales, aplicaciones móviles, redes sociales digitales, motores de búsqueda y uso de asistentes virtuales es indispensable definir la privacidad digital como el derecho que tiene cualquier usuario en la web a decidir cuáles datos personales desea compartir y quiere mantener resguardados para proteger la intimidad. La cuestión de la privacidad en internet implica realizar algunas tareas o compartir diferentes datos, como el nombre completo, dirección de domicilio, número de identificación personal, información bancaria, fotos, videos o audios personales, así como hacer compras en línea, transmitir geolocalización y utilizar servicios de atención al cliente de manera (chats, mensajes privados y correos electrónicos).

La privacidad de los usuarios de internet es parte de las políticas públicas de diversas organizaciones internacionales de las que México es parte; por ejemplo, la OCDE.[4]

La defensa de la privacidad evoca comprender que la protección de datos personales debe ser tratada de forma lícita y leal. Este principio es fundamental para enfrentar prácticas como la venta o transferencia de información personal obtenida fraudulentamente. La "lealtad y la transparencia" son esenciales para garantizar que los datos de las personas no se utilicen de manera inesperada. "Lícitos" significa que estos deben tratarse de manera que respete el Estado de derecho y que satisfaga un fundamento legal para el tratamiento.

4. Participación de México en la Organización para la Cooperación y el Desarrollo Económico. puede verse más información en el vínculo electrónico: http://www.oecd.org/mexico/

Apple, Facebook, Google y Microsoft se han autorregulado durante algún tiempo, a pesar de que estas compañías invierten fuertemente en la creación de poderosas tecnologías de reconocimiento facial. Facebook, por ejemplo, tiene un acuerdo con la Comisión Federal de Comercio (FTC) desde el año 2012,[5] por el cual la empresa primero debe obtener el "consentimiento expreso afirmativo" antes de ir más allá de la configuración de privacidad especificada por un usuario, sin embargo, fue insuficiente debido a que la compañía engaño a los usuarios al compartir información de sus contactos con desarrolladores de aplicaciones de terceros, aunque tuvieran su configuración de seguridad más detallada. Todo ello motivo que la FTC genere una nueva orden en el año 2019[6] con duración de 20 años resultando en compromisos para Facebook como la creación de un comité independiente de privacidad, enfocado en su vigilancia. A su vez, estableciendo responsabilidades a su CEO, Mark Zuckerberg, entre ellas, el revisar riesgos materiales y decisiones hechas trimestralmente en materia de privacidad y certificar a la compañía cumpliendo la nueva orden de la FTC como expandir su programa de transparencia incluyendo Instagram y Whatsapp.

Según investigadores en lo denominado como nuevo sistema arquitectónico online, se indica que el *DeepFace,* es un sistema de reconocimiento facial de Facebook, es 97,35 por ciento preciso debido a que emplea nueva capas con más de 120 millones de conexiones (Taigman et al, 2014:1). Eso se compara con 85 por ciento del sistema de identificación del FBI denominado *Next Generation Identification* (www.fbi.gov/services), lo cual advierte retos ante la función adecuada de los algoritmos y código que frene la comercialización de la información personal y sensible, al igual que la consagración de un modelo de vigilancia corporativa que tenga como fin un panóptico digital.

V.1. Datos personales post mortem

DLa defensa no sólo es dentro de la estructura tradicional de los datos personales, es decir, no solamente en vida existe daño a nuestra persona sino también posterior a la muerte, ¿a qué se debe? En gran medida al analfabetismo digital, a la intrusión tecnológica y su dependencia.

Generar conciencia sobre el valor económico que tienen los datos personales es fundamental debido a que cada punto general o específico ha sido expresado por el ciudadano en el andar cotidiano de uso de redes sociales digitales, mercados electrónicos y páginas web, por tal motivo, el Estudio hecho de la Asociación de Internet (2021) en México dio a conocer el monto de cada una de las informaciones

- Cantidad de hijos: 191.00 pesos.
- Domicilio: 230.00 pesos.
- Teléfono celular: 291.00 pesos.
- Registro Federal de Contribuyentes (RFC): 204.00 pesos.
- Tipo de Sangre: 158.00 pesos.

5. Véase: Acuerdo de la FTC con Facebook. https://www.ftc.gov/es/noticias/2019/07/la-ftc-impone-penalidad-de-5-mil-millones-y-nuevas-restricciones-de-privacidad-de Consultado: 17/11/2021
6. Véase: Hoja Informativa sobre la Orden del 2019 de la FTC con Facebook. https://www.ftc.gov/es/system/files/attachments/press-releases/la-ftc-impone-penalidad-de-5-mil-millones-y-nuevas-restricciones-de-privacidad-de-gran-envergadura/2019_order_fact_sheet_facebook_spanish.pdf Consultado: 17/11/2021

- Cuentas bancarias: 227.00 pesos.
- Perfil de red social digital, Facebook: 149 dólares.
- Perfil de red social digital, twitter: 32.5 dólares.
- Cuenta de mercado electrónico, Amazon: 375 dólares.[7]

Existen lagunas importantes en el marco jurídico de las leyes especiales sobre la protección de datos personales; por ejemplo, en el ejercicio de los derechos ARCO, por persona distinta a su titular o a su representante, o bien, respecto de información privados de personas fallecidas, ello no se encuentra previsto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y la normatividad que de ella deriva. Tampoco existe disposición legal alguna que regule el derecho a la protección de datos de personas fallecidas con motivo de su tratamiento por parte de los particulares.

Lo anterior, es totalmente distinto en lo establecido en el artículo 49, párrafo segundo, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, que sí considera el ejercicio de los derechos ARCO por persona distinta a su titular o a su representante, será posible, excepcionalmente, en aquellos supuestos previstos por disposición legal, o en su caso, por mandato judicial.

Al tratar los datos personales concernientes a personas fallecidas, el artículo 49, último párrafo, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, indica que la persona que acredite tener un interés jurídico, de conformidad con las leyes aplicables, podrá ejercer los derechos ARCO, siempre que el titular de los derechos hubiere expresado fehacientemente su voluntad en tal sentido o que exista un mandato judicial para dicho efecto.

En México, entro en vigor a partir del 1 de octubre de 2018 el "Decreto Promulgatorio del Protocolo Adicional al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las Autoridades de Control y a los Flujos Transfronterizos de Datos, el cual fue hecho en Estrasburgo, Francia, el 8 de noviembre de 2001.

El Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y su Protocolo Adicional no contempla distinción o restricción alguna sobre de los derechos o el tratamiento de la información privada de las personas fallecidas; sin embargo, no debería constituir un impedimento a la falta de previsión en las leyes secundarias para aplicar y reconocer el derecho de quienes manifiestan un interés jurídico o legítimo, en relación con los titulares.

Es primordial que el poder Legislativo federal fortalezca la homologación de regular el ejercicio de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) y disuelva también las discrepancias en la protección de datos

7. Véase Los datos personales después de la muerte. Tenorio Cueto, Guillermo A. El Economista. https://www.eleconomista.com.mx/opinion/Los-datos-personales-despues-de-la-muerte-20210520-0108.html

privados de personas fallecidas para brindar seguridad y certeza jurídica tanto a los responsables del tratamiento como a los titulares.

VI. Comentarios y análisis de protección de datos personales en México

PEn México se desempeñó una controversia a luz de diferentes representantes del poder Legislativo, expertos, académicos e integrantes de la ciudadanía tras la entrada en vigor del decreto (publicado en *Diario Oficial de la Federación*) a la Ley de Federal de Telecomunicaciones y Radiodifusión, donde se reforma y adiciona a los artículos 15, fracción XLII bis, 176 y 180 bis a 180 septimus, por lo que se crea la obligación de dar datos biométricos a todos los que tengan o adquieran una línea móvil e inicia la construcción del Padrón Nacional de Usuarios de Telefonía Móvil (Panaut).

Haciendo una brevísima síntesis de lo anterior, la senadora de Morena, Lucía Meza, presidenta de la Comisión de Comunicaciones y Transportes de la LXIV Legislatura en el Senado de la República, en abril del año 2021 presentó y comentó un dictamen para reformar la ley en materia de telecomunicaciones para reducir los delitos de extorsión y secuestro, que dejan ganancias a la delincuencia organizada estimadas en doce mil millones de pesos anuales.

Pese a lo negativo que resulta el tema este tiene diversos aspectos positivos, el más importante que hizo a la sociedad mexicana es reflexionar sobre el valor de sus datos personales e investigar el avance actual en materia de transparencia y tutela de la información personal.

Desde julio de 2007 se reformo el artículo 6° de la Constitución Política de los Estados Unidos Mexicanos, donde se define el mecanismo de acceso y rectificación de datos personales, así como las características del órgano ante el cuál se substanciarán los procedimientos de revisión que garanticen a las personas cada uno de estos derechos. Posteriormente, el 30 de abril de 2009 se reformo el artículo 73°, fracción XXIX-0, de la propia carta magna y otorgó la facultad al Congreso de la Unión a legislar en materia de protección de datos personales en posesión de particulares.

Sin embargo, las reformas continuarían en 2009. El 1 julio se haría una adición al artículo 16 de la ley fundamental, al reconocer como derecho la protección de datos personales y el 7 de febrero de 2014 se realizaría la reforma al artículo 6, fracción VIII, al poner la autonomía constitucional del organismo garante y las bases para ley general.

Todo lo anterior demuestra que es una falacia el espíritu de la reforma propuesto por la senadora, y más cuando se hace memoria sobre los documentos en los que es parte México, como el Convenio 108 del Consejo de Europa en materia de protección de datos personales y el Tratado Comercial entre México,

Estados Unidos de Norteamérica y Canadá (T-MEC), que contraviene en varios de sus capítulos; por ejemplo, el XVIII sobre Telecomunicaciones, también el XIX de Comercio Digital, entre otros.

VI.1. Inconstitucionalidad de la reforma a la Ley Federal de Telecomunicaciones y Radiodifusión

Entre los argumentos destacan los contenidos en la Ley Federal de Protección de Datos Personales en Posesión de Particulares (2010), que comprenden los principios de tutela en su capítulo II, artículo sexto, a saber:

> Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.[8]

Explicando brevemente cada principio se encuentra el derecho humano a proteger y defender la protección de datos personales

1. Licitud. Refiere al compromiso que deben asumir los entes privados tanto personas físicas como jurídicas que traten la información cuando se solicita la prestación de un bien o servicio, al configurar en el compromiso un voto de confianza en el buen uso de la información privada.
2. Consentimiento. Permite decidir de manera informada, libre, especifica e inequívoca si se desea compartir información con otras personas y qué información podrá compartir el individuo.
3. Calidad. Los datos proporcionados y calificados como personales deben ser correctos, exactos y completos y estar actualizados mientras se proporcione el servicio acordado con la empresa.
4. Información. Refiere a la potestad que te otorga la Ley de conocer previamente las características esenciales del tratamiento a los que serán sometidos los datos personales que se proporcionan a entes privados o empresas.
5. Proporcionalidad. Implica que quienes tratan datos personales deben recabar sólo lo necesario acorde con los fines expresos del servicio proporcionado.
6. Responsabilidad. Las personas físicas o morales deben garantizar dentro o fuera de México el cumplimiento con los principios esenciales de protección de datos personales y a rendir cuentas, en caso de algún incumplimiento.

Dicha reforma vulnera los siguientes conceptos constitucionales y convencionales:

- Los artículos 8, numeral 2 y 11, numeral 2, de la Convención Americana de los Derechos Humanos.
- Artículo 11, numeral 1, de la Declaración Universal de Derechos

8. Véase en: Ley Federal de Protección de Datos Personales en Posesión de Particulares (2010). http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Humanos.

- Artículo 14, numeral 2 y Articulo 19, del Pacto Internacional de Derechos Civiles y Políticos.

La reforma se encuentra inactiva para sus efectos en la creación del Padrón Nacional de Usuarios de Telefonía Móvil, así como la necesidad del usuario de proporcionar sus datos biométricos (como la iris, huella dactilar, voz…) a las empresas de telefonía móvil para tener acceso a su derecho humano a la comunicación, previsto en el artículo sexto de la carta magna.

El Instituto Federal de Telecomunicaciones y Radiodifusión, (IFT) comprometido por la reforma para generar tan aberrante labor designada por la ley vigente, rechazo contundentemente sus efectos y fue congruente a la génesis de su objeto, que es el desarrollo eficiente de las telecomunicaciones y la radiodifusión, conforme a lo dispuesto en la constitución y las leyes para regular, promover y supervisar el uso, aprovechamiento y explotación del espectro radioeléctrico, las redes y la prestación de los servicios de telecomunicaciones y la radiodifusión en México.

Además, el 16 de diciembre de 2020, el IFT aprobó el nuevo marco estratégico con el firme propósito de facilitar el desarrollo del ecosistema digital desde una visión integral y colaborativa, que coadyuve al desarrollo socioeconómico.

Por esa razón, resulta de reconocimiento la defensa del Estado derecho y a la naturaleza del organismo constitucional autónomo en cuestión mediante la controversia constitucional, presentada por el comisionado presidente Adolfo Cuevas Trejo, el 26 de mayo de 2021, contra diversas disposiciones contenidas en el decreto por el que se ordena al IFT a instalar, operar, regular y mantener el Padrón Nacional de Usuarios de Telefonía Móvil, bajo el argumento de cómo el Congreso de la Unión invadió su autonomía presupuestaria, así como sus facultades regulatorias y garantes de derechos humanos, ello generando una afectación a su garantía institucional y autonomía y transgredió el principio de división de poderes.

Asimismo, se expone, dentro del Comunicado 46/2021 del IFT, que no se dispone con los recursos para cumplir el mandato legislativo de poner en marcha el registro del Panaut con cargo a su presupuesto.[9]

VII. Conclusión

La privacidad de los usuarios constituye una variable fundamental en tales procesos técnicos como la obligación de configuraciones de seguridad, la modificación y actualización de certificados SSL (validación de que un sitio web es seguro) y contraseñas a rede sociales digitales, así como el rechazo al llenado de formularios que recolecten datos personales; además de procesos legislativos

9. Véase en: (Comunicado 46/2021) 26 de mayo. Instituto Federal de Telecomunicaciones y Radiodifusión. http://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/el-ift-interpuso-hoy-controversia-constitucional-en-contra-de-diversas-disposiciones-del-decreto-por

donde las reformas al Código Penal Federal robustezcan a quienes realicen delitos informáticos (esto a partir de su artículo 211 bis), en virtud de los riesgos que implican tanto por posibles ataques informáticos que puedan ocasionar un perjuicio patrimonial como en función de la representación de los sujetos en los espacios virtuales (Pérez, G. 2016).

Cabe precisar la necesidad de que los poderes del Estado defiendan la progresividad de los derechos humanos plasmados en la carta magna, y en armonía con los tratados internacionales, para aplicar una verdadera estrategia digital nacional que contemple la democratización del conocimiento técnico y jurídico.

Queda claro que la ruta en la defensa de la privacidad requiere de un mejor involucramiento de la sociedad, autoridades e iniciativa privada, pues la privacidad es multidimensional y cada día resulta más difícil armonizar cada uno de sus rubros, cabe recalcar la reflexión compartida por Habermas (2009) sobre la privacidad colectiva al plantear una relación de lo privado con lo público, que resulta muy fructífero para comprender el carácter individualista, pues es, en este ámbito, donde se producen las relaciones sociales (privadas) con relevancia pública y que desembocan en la creación de un espacio público en el que se forja la opinión pública.

VIII. Referencias bibliográficas

ANITUA, GABRIEL (2005) "'¡Identifíquese!' Apuntes para una historia del control de las poblaciones". p. 16, *http://www.pensamientopenal.com.ar/doctrina/30892-identifiquese-apuntes-historia-del-control-poblaciones*

A. LERVASI, C. VÁZQUEZ, D. ARCONDO et al., Informe Central Identificación Biométrica. Revista RNDS, No 20 Septiembre 2005, pp. 48 68, *http://www.rnds.com.ar/articulos/020/RNDS_048W.pdf*

DESANTES GUANTER, J.M.: "Intimidad e información, derechos excluyentes", Nuestro tiempo, 1972, núm. 213.

HABERMAS, J. (2009). Historia y critica de la opinión pública. Barcelona, España: Gustavo Gili. (Original publicado en 1990).

JAIN, A., BOLLE, R., PANKATI, S. (1996). *Introduction to biometrics* . En Biometrics. Boston: Springer.

PÉREZ, G. (2016). La privacidad en la sociedad del conocimiento: Reflexiones hacia una agenda educativa. *Revista Mexicana de Comunicación,* 1 (139), pp. 31-39.

R. SANCHEZ REILLO, C. SANCHEZ AVILA, J.A. MARTIN PEREDA., Minimal Template Size for Iris Recognition. Proc. of the First Joint BMES/EMBS

Conference. Atlanta (EE.UU.), 1316 Octubre, 1999. p. 972

RODRÍGUEZ, ANTONIO. La problemática de la biometría como método de autenticación. INCIBE, 2013. (Consultado: 11/10/2021) *https://www.incibe-cert.es/blog/problematica-biometria-autenticacion*

TORNABENE, Inés, "Privacidad e intimidad: la protección legal de la información personal en la República Argentina", en AMOROSO FERNÁNDEZ, Y., (dir.), Género, Código de Juventud: construir sociedades más justas e inclusivas, Unión Nacional de Juristas de Cuba, 2014, pp. 85-101.

TENORIO CUETO, GUILLERMO A. Los datos personales después de la muerte. El Economista. *https://www.eleconomista.com.mx/opinion/Los-datos-personales-despues-de-la-muerte-20210520-0108.html*

TAIGMAN, Y.; YANG, M.; RANZATO, M. Y WOLF, L. DeepFace: Closing the Gap to Human- Level Performance in Face Verification, 2014. In Conference on Computer Vision and Pattern Recognition (CVPR) Facebook Research. Véase: *https://research.facebook.com/publications/deepface-closing-the-gap-to-human-level-performance -in-face- verification*

UMANICK, *Timeline de la Biometria,* UMANICK LABS, S.L., 2014.

WESTIN, A. (1967): Privacy and freedom. New York: Athenaeum, p. 369.

WANG, Y., KOBSA, A. (2009). *Privacy enhancing technologies.* En Handbook of research on social and organizational liabilities in information security. Hershey: IGI Global Recuperado de https://bit.ly/2XF0gby

LAS DIRECTRICES PLANTEARON LOS PRINCIPIOS: DE LIMITACIÓN DE RECOGIDA DE DATOS PERSONALES; DE CALIDAD DE LOS DATOS PERSONALES. Véase en: *www.oecd.org/sti/ieconomy/15590267.pdf*

PARTICIPACIÓN DE MÉXICO EN LA ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICO (OCDE) Véase en: *http://www.oecd.org/mexico/*

DECRETO por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones y Radiodifusión. DOF: 16/04/2021. Véase en: *https://dof.gob.mx/nota_detalle.php?codigo=5616165&fecha=16/04/2021*

ACUERDO DE LA FTC CON FACEBOOK. Véase: *https://www.ftc.gov/es/noticias/2019/07/la-ftc-impone-penalidad-de-5-mil-millones-y-nuevas-restricciones-de-privacidad-de Consultado: 17/11/2021*

HOJA INFORMATIVA SOBRE LA ORDEN DEL 2019 DE LA FTC CON FACEBOOK. Véase. *https://www.ftc.gov/es/system/files/attachments/press-*

releases/la-ftc-impone-penalidad-de-5-mil-millones-y-nuevas-restricciones-de-privacidad-de-gran-envergadura/2019_order_fact_sheet_facebook_spanish.pdf Consultado: 17/11/2021

FBI SERVICES. NEXT GENERATION IDENTIFICATION (NGI), Véase: *https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi* Consultado: 17/11/2021