

REVISTA EUROLATINOAMERICANA DE DERECHO ADMINISTRATIVO

VOL. 8 | N. 1 | ENERO/JUNIO 2021 | ISSN 2362-583X
SANTA FE | ARGENTINA | PERIODICIDAD SEMESTRAL

Revista oficial de la Red Docente Eurolatinoamericana de Derecho Administrativo
formada por las siguientes instituciones:



RED DOCENTE
EUROLATINOAMERICANA
DE DERECHO ADMINISTRATIVO



El derecho a la privacidad y la protección de datos personales transfronterizos

The right to privacy and the protection of personal data across borders

ANA GLORIA ROBLES OSOLLO I.*

^I Universidad Nacional Autónoma de México (Acatlán, México)

agrobleso@gmail.com

<https://orcid.org/0000-0001-9502-3165>

Recibido el/Received: 25.01.2021 / January 25th, 2021

Aprobado el/Approved: 13.04.2021 / April 13th, 2021

RESUMEN:

El derecho humano a la privacidad y el manejo de los datos personales transfronterizos, demanda la máxima protección frente al intercambio de información que se desarrolla entre los distintos países por diversos temas, como la salud, la política, el comercio y por el uso de las nuevas tecnologías, así como, la posible colisión con el derecho al acceso a la información. Analizar el tratamiento y normativa europea, así como, la recepción normativa mexicana como país latinoamericano de vanguardia y firmante del Convenio 108 de Estrasburgo es de la mayor importancia.

Palabras clave: datos personales; datos sensibles; flujos transfronterizos; instrumentos internacionales; Convenio 108 de Strasburgo.

ABSTRACT:

The right to privacy and the transnational personal data, urge the legal systems for and adequate protection, the information exchange between countries, such as health, politics, trade and the use of new technologies, as well as the possible collision with the right of access to information. The analysis of the European regulations to protect data, as well as the reception of Mexican regulations as a leading Latin American country and a signatory of the Convention 108 of Strasbourg is paramount.

Keywords: personal data; sensitive data; cross-border flows; international instruments; economic data; Convention 108 of Strasbourg.

Como citar este artículo | *How to cite this article:* ROBLES OSOLLO, Ana Gloria. El derecho a la privacidad y la protección de datos personales transfronterizos. **Revista Eurolatinoamericana de Derecho Administrativo**, Santa Fe, vol. 8, n. 1, p. 35-60, ene./jun. 2021. DOI 10.14409/redoeda.v8i1.9543.

* Fundadora de la Unidad de Posgrado en Derecho de la Universidad Nacional Autónoma de México – UNAM (Acatlán, México). Doctora y Licenciada en Derecho por la Universidad Nacional Autónoma de México. Máster Universitario en Protección Internacional de los Derechos Humanos por la Universidad de Alcalá de Henares (Alcalá, España). Especialista en Derechos Humanos por la Universidad de Castilla-La Mancha (Toledo, España). Especialista en Desarrollo Humano por el Instituto Humanista de Psicoterapia Gestalt (IHPG). E-mail: agrobleso@gmail.com.



SUMARIO:

1. Introducción; **2.** Antecedentes; **3.** Documentos internacionales que abordan el tratamiento y significado del flujo de datos transfronterizo; **4.** Caso de México. Marco jurídico y la importancia de un adecuado tratamiento de los flujos de datos transfronterizo enfocado a la administración pública; **5.** Los riesgos ante la innovación tecnológica mediante el análisis de la ética en el uso de las nuevas tecnologías; **6.** Conclusiones; Referencias.

1. INTRODUCCIÓN

La protección jurídica de datos personales es un fenómeno global, que desde los años setenta se ha incrementado en forma exponencial para regular la transferencia de datos, impulsada por los rápidos avances tecnológicos, comerciales y financieros que agregan un valor económico y social significativo a los mismos.

A la par, observamos que la interdependencia económica entre las naciones resulta irreversible, por lo que el interés por una mayor protección del derecho humano a la privacidad de las personas y sus libertades individuales se vuelve prioritario.

La vulneración de los datos personales está estrechamente vinculado con el derecho a la privacidad, lo que hace que la protección a los datos personales sea controvertible frente al derecho a la privacidad y al derecho al acceso a la información, sobre todo tratándose de servidores públicos, lo que ha implicado una difícil ponderación de derechos frente a la universalidad, interdependencia, indivisibilidad y progresividad de los derechos humanos como lo marca el artículo 1° de la Constitución Política de los Estados Unidos Mexicanos¹. La posible colisión de derechos y su ponderación por señalar algunos, son: la dignidad de la persona, la vida, la igualdad, la integridad, la vida privada, la intimidad, la seguridad, la salud, el acceso a la información, entre otros. Esta vulneración no se da solamente a nivel nacional, sino que el flujo de los datos personales se transmigran a nivel internacional, lo que nos vuelve más vulnerables y cada día más expuestos a distintos intereses, ya sean políticos, económicos, de salud, sociales, publicitarios, migratorios y delictivos entre otros.

La Comisión Nacional de los Derechos Humanos de México define en su página web, a los derechos humanos como “el conjunto de prerrogativas sustentadas en la dignidad humana, cuya realización efectiva resulta indispensable para el desarrollo integral de la persona.”² Lo que podemos traducir en general, como ese conjunto de

¹ MEXICO. Cámara de Diputados. **Constitución Política de los Estados Unidos Mexicanos**. 5 de febrero de 1917. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf_mov/Constitucion_Politica.pdf Acceso del 15 de agosto del 2020.

² MEXICO. COMISIÓN NACIONAL DE LOS DERECHOS HUMANOS. **Que son los derechos humanos**. Disponible en: http://www.cndh.org.mx/Que_son_derechos_humanos Acceso el 15 de agosto del 2020.



derechos que hacen factible el progreso y adelanto de las niñas, niños, adolescentes y personas desde su condición en diversas áreas de su vida, para lograr autodeterminación y libre toma de decisiones para acceder en igualdad de oportunidades a esos derechos que el Estado otorga, promueve y protege. Cabe destacar que no se debe olvidar que no solo existen derechos, sino también **deberes** humanos como lo previene la Declaración Americana de los Derechos y Deberes del Hombre de fecha 2 de mayo de 1948, en los artículos XXIX al XXXVIII, que forma parte del Sistema Americano y que precedió a la Declaración Universal de los Derechos Humanos que pertenece al Sistema de Naciones Unidas.

Ante este panorama, la colaboración internacional se hace obligatoria, tanto por el tema jurisdiccional, como por el aspecto normativo y de seguridad. Ello resulta fundamental para poder generar confianza y tranquilidad en las personas, en el sentido de que los países están trabajando en proteger la intimidad de los datos personales de sus connacionales, y que no se haga un uso indebido de la información personal que pueda generar daños irreparables.

El fenómeno del flujo de datos transfronterizo es hoy en día, un verdadero desafío para el Derecho y para la sociedad misma; por una parte, existe la necesidad de equilibrar el interés público respecto a estos datos y por la otra, velar por el respeto a los derechos fundamentales de la persona titular de dicha información. México sin duda es hoy un referente legislativo importante en el avance del tema de protección jurídica del flujo de datos transfronterizo. Sin embargo, se desprende la siguiente interrogante.

¿Cuáles con los antecedentes de protección a la vida privada y de los datos personales?

2. ANTECEDENTES

La protección de la vida privada, es considerado de primera generación por su aparición histórica más remota, uno de los primeros derechos que fueron exigidos al Estado Absolutista, así como, derechos de no intervención ni injerencia en la vida privada, ni en el domicilio, ni a la correspondencia. A partir de la segunda guerra mundial, se pudo atestiguar como era poco el avance de la humanidad y como ésta era capaz de cometer los más horribles crímenes en contra de las personas, así como violaciones generalizadas y sistemáticas de los derechos humanos, lo cual sirvió de base para un nuevo orden mundial a partir del cual surgen Instrumentos Internacionales importantes para la protección del derecho a la vida privada de las personas entre los cuales destacan:

- a) **La Declaración Americana de los Derechos y Deberes del Hombre** del 2 de mayo de 1948 en el artículo V. Derecho a la protección a la honra, la reputación personal y la vida privada y familiar y precisaba: "Toda persona tiene derecho a



la protección de la ley contra los ataques abusivos en su honra, a su reputación y a su vida privada y familiar.”; (Sistema Americano)

- b) La Declaración Universal de los Derechos Humanos** del 10 de diciembre de 1948, un catálogo de 30 derechos a partir de los cuales se formulan y desarrollan Pactos, Convenciones y demás Instrumentos Internacionales que forman parte del contenido constitucional de numerosos países democráticos. Y en seguimiento a los antecedentes, encontramos en el artículo 12 lo siguiente: “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataque a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley entra tales injerencias o ataques.”(Sistema de Naciones Unidas, no vinculante)
- c) Pacto Internacional de Derechos Civiles y Políticos** de 16 de diciembre de 1966, suscrito por México en 1981, reconoce en su artículo 17 que “1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.” (Sistema de Naciones Unidas)
- d) Convención Americana sobre Derechos Humanos** del 22 de noviembre de 1969, suscrito por México en 1981, (Pacto de San José) reconoce en su artículo 11, la Protección de la Honra y de la Dignidad y señala en el numeral 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. “Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni ataque ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques” (Sistema Americano)
- e) Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales** de fecha 4 de noviembre de 1950. En su artículo 8 del Derecho al respeto a la vida privada y familiar, señala “1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la **seguridad nacional**, el **bienestar económico del país**, la defensa del orden y la prevención del delito, **la protección de la salud** o de la moral, o la protección de los derechos y las libertades de los demás.” (Sistema europeo)
- f) Carta de los Derechos Fundamentales de la Unión Europea.** Año 2000, prevé en su artículo 7 Respecto de la vida privada y familiar lo siguiente: “Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones”. (Sistema europeo, no vinculante)



Sin embargo al ser un texto más reciente, ya prevé en su artículo 8, el tema de la Protección de Datos de Carácter Personal y señala textualmente:

- 1) Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
- 2) Estos datos se tratarán de modo leal, para fines concretos y sobre la base del conocimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
- 3) El respeto a estas normas quedará sujeto al control de una autoridad independiente.

Este último documento constituye un claro antecedente del derecho humano a la protección de datos personales, en el cual, a su vez destaca la regulación que cada país desarrolla en la temática, haciendo la mejor ponderación jurídica de los derechos humanos para evitar la afectación de las personas en la transmigración de sus datos personales.

En el contexto nacional, México no ha sido la excepción, en la protección de la vida privada y de los datos personales como líneas adelante esquematizaremos, pero no sin antes consultar y referir, otro tipo de documentos internacionales, específicos y fundantes para el universo de significado que hoy tiene el derecho humano a la protección de datos personales, por lo que resulta conveniente responder a la pregunta de ¿Cuál es el marco de protección internacional para los datos personales desde la óptica de los derechos humanos con la figura de datos transfronterizo?

3. DOCUMENTOS INTERNACIONALES QUE ABORDAN EL TRATAMIENTO Y SIGNIFICADO DEL FLUJO DE DATOS TRANSFRONTERIZO

Al analizar, los documentos internacionales que abordan el tratamiento del flujo de datos transfronterizo, resulta insoslayable la revisión de cinco documentos fundantes en el ámbito a internacional, siendo estos:

- 1) Las “Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales”³, de fecha 23 de septiembre de 1980;
- 2) La Directiva 95//46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, que ya ha sido derogada.
- 3) El Convenio No. 108 del Consejo de Europa denominado, “Convenio para la Protección de las personas con respecto al tratamiento automatizado de datos de

³ FRANCIA. Organización para la Cooperación Económica Europea. **Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales**. 23 de septiembre de 1980. Disponible en: http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf Acceso el 15 de agosto de 2020.



- carácter personal”⁴, de fecha 28 de Enero de 1981 que construye su contenido a partir de las importantes resoluciones del Consejo de Europa de 1973 y 1974⁵, y
- 4) El “Protocolo Adicional relativo a las autoridades de control y a los flujos transfronterizos de datos”⁶, de fecha 8 de noviembre de 2001.
 - 5) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

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

Estas Directrices son los primeros esfuerzos por sistematizar un tratamiento específico sobre un tema que se venía desarrollando décadas atrás por la OCDE⁷, o la OECD⁸ *Organisation of Economic Co-operation and Development*, quien publica las primeras pautas para regular la protección de la privacidad y el flujo transfronterizo de datos personales en 1980.

De esta importante Organización (OCDE) integrada 37 países, tres son latinoamericanos: México, Chile y Colombia, y actualmente están en espera de ser aceptados también; Perú, Costa Rica, Argentina y Brasil⁹.

⁴ MEXICO. Instituto Nacional de Transparencia, Acceso a la información y protección de Datos Personales. **Convenio 108 del Consejo De Europa, para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de carácter personal.** 28 de Enero de 1981. Disponible en: <http://inicio.ifai.org.mx/Estudios/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf> Acceso el 15 de agosto de 2020.

⁵ MOLET, Jorge. El Economista. . **Adopción de México del Convenio 108 del Consejo de Europa, protección y flujo internacional de datos.** 20 de junio de 2018. Disponible en: <https://www.eleconomista.com.mx/opinion/Adopcion-de-Mexico-del-Convenio-108-del-Consejo-de-Europa-proteccion-y-flujo-internacional-de-datos-20180620-0098.html> Acceso el 15 de agosto de 2020.

⁶ FRANCIA. Consejo de Europa. **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.** 8 de noviembre de 2001. Disponible en: <https://rm.coe.int/16806c1abe> Acceso el 15 de agosto de 2020.

⁷ Cfr. Organización para la Cooperación y el Desarrollo Económicos (OCDE) Fundada en 1961, agrupa a 37 países miembros y su misión es promover políticas que mejoren el bienestar económico y social de las personas alrededor del mundo. Disponible en: <https://www.oecd.org/centrodemexico/laocde/> Acceso el 15 de agosto de 2020.

⁸ Cfr. Organización para la Cooperación Económica Europea (OCEE) 1948. con el propósito de dirigir el Plan Marshall financiado por Estados Unidos para reconstruir un continente devastado por la guerra. Al hacer que los gobiernos reconocieran la interdependencia de sus economías, se preparó el terreno para una nueva era de cooperación que habría de cambiar la faz de Europa. Alentados por su éxito y por la perspectiva de trasladar su trabajo a un escenario mundial, Canadá y Estados Unidos se unieron a los miembros de la OCEE al suscribir la nueva Convención de la OCDE el 14 de diciembre de 1960. La Organización para la Cooperación y el Desarrollo Económicos (OCDE) nació oficialmente el 30 de septiembre de 1961, cuando la Convención entró en vigor. Disponible en: <http://www.oecd.org/centrodemexico/laocde/historia-ocde.htm> Acceso el 15 de agosto de 2020.

⁹ MORALES, Yolanda. La OCDE está lista para fortalecer tributación de empresas digitales. **El Economista.** 23 de mayo de 2019. Disponible en: <https://www.eleconomista.com.mx/economia/La-OCDE-esta-lista-para-fortalecer-tributacion-de-empresas-digitales-20190523-0078.html> Acceso el 15 de agosto de 2020.



La OCDE tiene como propósito el coordinar y armonizar políticas económicas y sociales para intercambiar información con el objetivo de expandir el desarrollo y crecimiento económico entre los países miembros y no miembros, por lo que se destaca que la OCDE agrupa a los países que representan entre el 60% y 70 % del mercado mundial. Lo que trae implicaciones importantísimas tratándose de intercambio de flujo de datos transfronterizo.

La OCDE reúne a un grupo de países con ideas similares. Esencialmente, el ser miembro de la organización depende del compromiso de un país hacia la economía de mercado y la democracia pluralista. Es una organización próspera ya que sus treinta y siete países miembros producen el 60% de los bienes y servicios del mundo, pero no es de ninguna manera una organización exclusiva. A los países no miembros se les ha invitado a suscribirse a acuerdos y tratados de la OCDE. Así mismo, la Organización comparte sus experiencias y puntos de vista en temas de interés mutuo con más de 70 países como Brasil, China y Rusia y con otros países menos desarrollados de África.¹⁰

Comprender la importancia de esa Organización y su liderazgo, resulta sustancial para México y Latinoamérica, en el tema de flujo de datos transfronterizos, considerando que en el mes de enero de 2016, crean el “Programa Regional de la OCDE para América Latina y el Caribe¹¹, que fue renovado recientemente para un segundo ciclo de tres años (2019-2022).

Con la elaboración de las Directrices emitidas por la OCDE, se establecen normas mínimas para la protección de la privacidad y el flujo transfronterizo de datos personales, desde el 23 de septiembre de 1980, con una clara preocupación sobre la exposición de la privacidad de las personas frente a la transferencia de datos personales que circulen en los países y su adecuado tratamiento en el ámbito público y privado, que no pueden de ninguna manera desvincularse.

Las Directrices consideran, como excepciones a la vulneración al derecho humano a la privacidad y a las libertades individuales: la soberanía nacional, la seguridad nacional y la política pública de los Estados, regulación que debe ser adicionada a la

¹⁰ Cfr. Organización para la Cooperación y el Desarrollo Económicos. Alemania, Australia, Austria, Bélgica, Canadá, Chile, Colombia, Corea, Dinamarca, Eslovenia, España, Estados Unidos, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Islandia, Israel, Italia, Japón, Letonia, Lituania, Luxemburgo, México, Noruega, Nueva Zelanda, Países Bajos, Polonia, Portugal, Reino Unido, República Checa, República Eslovaca, Suecia, Suiza, Turquía. Disponible en: <https://www.oecd.org/centrodemexico/laocde/masinformacionsobrelaocde.htm> Acceso el 15 de agosto de 2020.

¹¹ Cfr. Organización para la Cooperación y el Desarrollo Económicos. Alemania, Australia, Austria, Bélgica, Canadá, Chile, Colombia, Corea, Dinamarca, Eslovenia, España, Estados Unidos, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Islandia, Israel, Italia, Japón, Letonia, Lituania, Luxemburgo, México, Noruega, Nueva Zelanda, Países Bajos, Polonia, Portugal, Reino Unido, República Checa, República Eslovaca, Suecia, Suiza, Turquía. Disponible en: <https://www.oecd.org/centrodemexico/laocde/masinformacionsobrelaocde.htm> Acceso el 15 de agosto de 2020.



legislación específica de cada país para su tratamiento, pudiendo incluso imponer un país miembro restricciones en ciertas categorías de datos personales si su legislación domestica así lo considera, pero con la petición de elaborar legislación y prácticas que no sean obstáculo a los flujos transfronterizos de datos personales entre los Estados por un exceso en la regulación y protección del derecho a la privacidad y las libertades individuales.

El referido documento define como flujos transfronterizos de datos personales a “los desplazamientos de datos personales más allá de las fronteras nacionales”.¹²

Asimismo, las Directrices definen como datos personales a “toda información relativa a un individuo identificado o identificable (sujeto de los datos)” y al inspector de datos, como la “persona que, según la ley del país, es competente para decidir sobre el contenido y el uso de datos personales con independencia de si esos datos son, o no, recogidos, guardados, tratado o divulgados por esa persona o por un representante en su nombre.”

Desde la óptica inevitable de los derechos humanos, la OCDE previó en las Directrices los principios básicos nacionales e internacionales para la protección de los datos personales, que fueron recogidos el 28 de enero de 1981 en el Convenio no. 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su respectivo Protocolo Adicional de fecha 8 de noviembre de 2001, entrando ambos en vigor en México el 1 de octubre de 2018.¹³

Es por ello que estas Directrices son consideradas como un documento pionero y fundamental para la legislación que hoy se tiene, al prever como principios básicos: I. El principio de limitación de recogida, II. El principio de calidad de los datos, III. El principio especificación de los fines, IV. El principio de limitación de uso, V: El principio de salvaguarda de la seguridad, VI. El principio de participación individual, de responsabilidad y principio de transparencia.¹⁴

¹² Organización para la Cooperación y el Desarrollo Económicos. **Directrices de la OCDE que regulan la protección de la privacidad y el Flujo transfronterizo de datos personales.** 23 de septiembre de 1980. Disponible en: http://www.oas.org/es/sla/ddi/docs/directrices_ocde_privacidad.pdf Acceso el 15 de agosto de 2020.

¹³ MÉXICO. Diario Oficial de la Federación. **Decreto Promulgatorio del Convenio 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 mil novecientos ochenta y uno. 28 de septiembre de 2018. Y **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**, hecho en Estrasburgo, Francia, el ocho de noviembre de dos mil uno. 28 de septiembre 2018. Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5539473&fecha=28/09/2018. Acceso el 15 de agosto de 2020.

¹⁴ Cfr. Organización para la Cooperación y el Desarrollo Económicos. **Directrices de la OCDE que regulan la protección de la privacidad y el Flujo transfronterizo de datos personales.** 23 de septiembre de 1980. Disponible en: http://www.oas.org/es/sla/ddi/docs/directrices_ocde_privacidad.pdf. Acceso el 15 de agosto de 2020. PARTE SEGUNDA. PRINCIPIOS BÁSICOS DE APLICACIÓN NACIONAL. Principio de limitación de recogida 7. Debería haber límites a la recogida de datos personales y cualquiera de esos datos debería



Estos riesgos de alta implicación internacional han generado que numerosos organismos internacionales trabajen en una mayor regulación jurídica para la protección de datos de las personas, además de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), la Oficina Intergubernamental para la Información (OMP), el Centro de Corporaciones Transnacionales de las Naciones Unidas (UNCTAD), Banco Mundial, Foro Económico Mundial, por señalar solo algunos.

b) Directiva 95//46/CE del Parlamento Europeo y del Consejo de la Unión Europea 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 a partir del 25 de mayo de 2018.¹⁵

Esta directiva, destaca frente a la libre circulación de mercancías, personas, servicios y capitales de la Unión Europea, que es donde surge este interés con más fuerza para la protección de los datos personales por la gran actividad desarrollada, como el fortalecimiento de la cooperación científica y técnica, redes de telecomunicaciones, el aumento en el flujo transfronterizo de datos personales que pudieran tener distintos grados de protección que por la legislación interna, impidieran la transmisión de los mismos, obstaculizando el intercambio de actividades económicas, por lo que hace esta Directiva

ser obtenido por medios legales y honestos y, en su caso, con el conocimiento o consentimiento del sujeto de los datos. Principio de calidad de los datos 8. Los datos personales deberían corresponder a los fines para los que se van a usar y, en la medida en que sean necesarios para esos fines, deberían ser correctos y completos, y estar actualizados. Principio de especificación de los fines 9. Los fines para los que los datos personales se recogen deberían especificarse en el momento en que se recogen, y su uso posterior estaría limitado al cumplimiento de esos fines o de otros que no sean incompatibles con esos fines y se especifiquen cada vez que haya un cambio de fines. Principio de limitación de uso 10. Los datos personales no se deberían revelar, poner a disposición del público ni usar para fines que no sean los especificados de conformidad con el apartado 9 anterior, excepto: a) con el consentimiento del sujeto de los datos; o b) por imperativo legal. Principio de salvaguarda de la seguridad 11. Los datos personales deberían estar protegidos por las oportunas medidas de salvaguarda contra riesgos como pérdida o acceso no autorizado, destrucción, uso, modificación o revelación de datos. Principio de transparencia 12. Debería haber una política general de transparencia en lo concerniente al tratamiento, el uso y las políticas relativos a los datos personales. Se deberían poner los medios para establecer la existencia y la naturaleza de los datos personales, así como los fines principales para los que se van a usar, así como la identidad y el domicilio habitual del inspector de datos. Principio de participación individual 13. Toda persona física debería tener derecho a: a) conseguir, a través de un inspector de datos o de otra manera, la confirmación de si el inspector tiene o no tiene datos relativos a su persona; b) que se le comunique cualquier dato relativo a ella: 1. m en un plazo de tiempo razonable; m con una tarifa, en su caso, que no sea excesiva; m de manera razonable; y m de forma que pueda entender fácilmente; 2. c) que se le den las razones de porqué se rechaza una petición hecha de conformidad con lo establecido en los apartados (a) y (b), y poder recurrir ese rechazo; d) recusar los datos relativos a ella y, si la recusación tiene éxito, hacer que se eliminen, rectifiquen, completen o modifiquen los datos. Principio de responsabilidad 14. A todo inspector de datos se le deberían pedir responsabilidades por el cumplimiento de las medidas que permiten la aplicación de los principios antes expuestos.

¹⁵ BELGICA. Diario Oficial de la Unión Europea. **Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo**, 27 de abril de 2016. Disponible en: <https://www.boe.es/doue/2016/119/L00001-00088.pdf> Acceso el 15 de agosto de 2020.



95/46/CE¹⁶, un llamado a la armonización nacional con el propósito de garantizar el respeto de los derechos y libertades fundamentales y particularmente el derecho al respeto a la vida privada reconocido en el artículo 8 del Convenio Europeo que consta de 34 artículos para unificar el tema en la unión europea.

c) 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.

Este resulta ser el primer y único convenio internacional que a la fecha existe, al cual México se suscribe en el año 2018, iniciando su vigencia en territorio mexicano el 1 de octubre, recogiendo el Convenio gran parte de la información trabajada en las Directrices, y demás antecedentes, destacando y adicionando una aportación axiológica muy oportuna que deben guardar las partes, sin la cual sería mucho más compleja la tarea de la regulación y protección de los datos personales, de donde derivó el aspecto ético profesional como un binomio imprescindible para el éxito de esta temática al estar en prelación el interés común entre los países miembros para proteger el derecho a la vida privada principalmente y a las libertades individuales, cuando converjan o puedan entrar en colisión con otros derechos como sería el derecho al acceso a la información y el derecho a la transparencia.

Uno de los grandes temas indeterminados en materia de derechos humanos es la ponderación de éstos, su equilibrio y sus límites, ya que algunos derechos humanos son absolutos y otros relativos. Los derechos humanos y las libertades de todas las personas en su esencia contienen valores fundamentales esenciales que parecieran contradictorios o irreconciliables cuando entran en colisión como cuando se trata de la protección de los datos personales, el derecho a la vida privada, el derecho humano al libre acceso y circulación de la información, el derecho a la transparencia gubernamental.

Más allá de estas inquietudes, el Convenio sienta las bases para un mayor equilibrio para lo que resulta altamente conveniente la lectura puntual de los artículos 1° al 12° del Convenio, para conocer el objeto, el fin, definiciones importantes, para su aplicación, así como los principios básicos para la protección de datos y su tratamiento en los flujos de datos transfronterizos que sean acordes a la legislación nacional del Estado que se adhiera como Miembro.

En este orden de ideas, el artículo primero, refiere al objeto y fin, que garantiza a los Estados parte y a cualquier persona física, sin importar nacionalidad o residencia, el respeto de sus derechos y libertades fundamentales, privilegiando el derecho a la vida privada, en el tratamiento automatizado de los datos personales.

¹⁶ LUXEMBURGO. Parlamento Europeo. **Directiva 95/46/CE del Parlamento Europeo y del Consejo.**, 24 de octubre de 1995. Disponible en: EUR-Lex - 31995L0046 - EN - EUR-Lex (europa.eu) Acceso 10 de agosto de 2020.



El artículo segundo, hace referencia a la definición de **datos de carácter personal**, que los define como “cualquier información relativa a una persona física identificada o identificable”, muy similar a la definición de las Directrices y que para la legislación mexicana los define como Datos personales¹⁷.

Por **fichero automatizado**, se entenderá “cualquier conjunto de informaciones que sea objeto de un tratamiento automatizado”; **tratamiento automatizado**, será el registro de datos y la “aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión”; y la **autoridad** que controle el fichero, será “la persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo que sea competente con arreglo a la ley nacional para decidir cuál será la finalidad del fichero automatizado, cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les aplicarán”, que con mayor precisión regula el Protocolo Adicional del Convenio.

El artículo tercero, hace referencia al campo de aplicación para el tratamiento de los datos personales con las especificaciones y excepciones en los sectores públicos y privado, la ratificación, aceptación, aprobación o adhesión del Convenio haciendo de conocimiento al Secretario General del Consejo de Europa.

Los compromisos de las partes, están regulados en el artículo cuarto, en el que las partes se comprometen en su derecho interno, a tomar las medidas necesarias para hacer efectivos los principios básicos para la protección de datos previstos en el Convenio.

El artículo quinto prevé la calidad y legalidad en el tratamiento automatizado de los datos de carácter personal, identificables y por el tiempo necesario para cumplir con la finalidad de su registro. Lo que en México se conoce como derechos ARCO¹⁸.

El artículo sexto, resulta de especial relevancia, porque hace referencia a los conocidos en México como datos sensibles¹⁹, y que guardan un especial tratamiento, no

¹⁷ Cfr. MEXICO. Cámara de Diputados. **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados**. 26 de enero de 2017. Disponible en: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf>.

¹⁸ MEXICO. Cámara de Diputados. **Constitución Política de los Estados Unidos Mexicanos**. 5 de febrero de 1917. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf_mov/Constitucion_Politica.pdf Acceso del 15 de agosto de 2020. Artículo 16 párrafo segundo. “Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.” MEXICO. Cámara de Diputados. **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados**. 26 de enero de 2017. Disponible en: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf> Acceso del 15 de agosto de 2020. Artículo 3 fracción XI. Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

¹⁹ Artículo 3 fracción X. Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual; Artículo 7. Por regla general no podrán



pudiendo ser automatizados, a menos que el derecho interno prevea garantías a los mismos. El convenio los denomina, **categorías particulares de datos**, y son aquellos que revelan “el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual”, incluyendo los datos de carácter personal referentes a condenas penales.

El artículo séptimo hace referencia al importante tema de la seguridad de los datos, que de acuerdo al Convenio deberán resguardarse ficheros automatizados que eviten “la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados”, que hoy conocemos como soportes electrónicos o base de datos informáticos. En México se conoce como Base de datos.²⁰

El octavo hace referencia a la responsabilidad del fichero automatizado o base de datos que garantice la protección de los datos personales, su existencia y el ejercicio de lo que en la legislación mexicana se conoce como los derechos ARCO²¹ y los recursos en caso de incumplimiento, y las excepciones y restricciones contempladas en el artículo noveno del Convenio hacen referencia a la seguridad del Estado, la seguridad pública, intereses monetarios del Estado, infracciones penales, que la legislación mexicana prevé, en el denominado Documento de seguridad.²²

tratarse datos personales sensibles, salvo que se cuente con el consentimiento expreso de su titular o en su defecto, se trate de los casos establecidos en el artículo 22 de esta Ley. En el tratamiento de datos personales de menores de edad se deberá privilegiar el interés superior de la niña, el niño y el adolescente, en términos de las disposiciones legales aplicables. Artículo 21 párrafo cuarto. Tratándose de datos personales sensibles el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca, salvo en los casos previstos en el artículo 22 de esta Ley.

Ley Federal de Protección de datos personales en posesión de los particulares. Art. 3 fracción VI. Datos personales sensibles: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual. Art. 9. Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado. <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>.

²⁰ Ley General de Protección de datos personales en posesión de sujetos obligados. Artículo 3. Fracción III. Bases de datos: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización; <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf>.

²¹ Artículo 3º, fracción XI de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

²² Cfr. MÉXICO. Cámara de Diputados. **Ley General de Protección de datos personales en posesión de sujetos obligados**. 26 de enero de 2017. Disponible en: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf> Acceso el 15 de agosto de 2020. Artículo 3. XIV. **Documento de seguridad**: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas



El artículo noveno, hace referencia a las excepciones y restricciones, y su correlativo adoptado en la legislación mexicana serían los artículos 22,65, 66 al 71 de la Ley General de Protección de Datos Personales en posesión de sujetos obligados que contempla transferencia de datos nacional e internacional garantizando la confidencialidad, la previsión del aviso de privacidad, con la responsabilidad de la protección de los datos personales por parte de los receptores, con las responsabilidades por incumplimiento, salvo razones de seguridad nacional, servicios sanitarios, investigación y persecución de los delitos, procuración y administración de justicia, previsiones de tratados o convenios internacionales ratificados por México principalmente²³.

El decimo artículo se refiere a las sanciones y recursos para las partes, remite a las disposiciones de derechos interno que den cumplimiento a lo establecido en los principios básicos de protección del convenio, cuyo articulado correlativo para México, lo prevé la Ley General que se comenta, en el capítulo II, denominado de las Sanciones, de los artículos 163 con XIV fracciones y supuestos específicos, al 168, fracciones que contemplan, el inadecuado o doloso tratamiento de los datos personales, el uso indebido de los derechos ARCO, no contar con aviso de privacidad o inadecuada previsión, ilegal transferencia de datos personales, falta de medidas de seguridad para la protección de datos personales, bases de datos sin medidas de seguridad y legales, principalmente.²⁴

adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee. **XX. Medidas de seguridad:** Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales; **XXI. Medidas de seguridad administrativas:** Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales; **XXII. Medidas de seguridad físicas:** Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades: a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información; b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información; c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad **XXIII. Medidas de seguridad técnicas:** Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades: a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados; b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones; c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

²³ MÉXICO. Cámara de Diputados. **Ley General de Protección de datos personales en posesión de sujetos obligados**. 26 de enero de 2017. Disponible en: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf> Acceso el 15 de agosto de 2020.

²⁴ MÉXICO. Cámara de Diputados. **Ley General de Protección de datos personales en posesión de sujetos obligados**. 26 de enero de 2017. Disponible en: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf> Acceso el 15 de agosto de 2020.



El decimo primer artículo hace referencia en la interpretación de la norma, a conceder a las personas en el tema de protección de datos la más alta prevista. Que para el caso de México lo prevé en el artículo 8 de la ley multicitada, que se transcribe:

La aplicación e interpretación de la presente Ley se realizará conforme a lo dispuesto en la Constitución Política de los Estados Unidos Mexicanos, los Tratados Internacionales de los que el Estado mexicano sea parte, así como las resoluciones y sentencias vinculantes que emitan los órganos nacionales e internacionales especializados, favoreciendo en todo tiempo el derecho a la privacidad, la protección de datos personales y a las personas la protección más amplia. Para el caso de la interpretación, se podrán tomar en cuenta los criterios, determinaciones y opiniones de los organismos nacionales e internacionales, en materia de protección de datos personales.

El artículo decimo segundo es de especial importancia por lo que se transcribe del capítulo III del Convenio y que a la letra dice:

Artículo 12. Flujos transfronterizos de datos de carácter personal y el derecho interno

1. Las disposiciones que siguen se aplicarán a las transmisiones a través de las fronteras nacionales, por cualquier medio que fuere, de datos de carácter personal que sean objeto de un tratamiento automatizado o reunidos con el fin de someterlos a ese tratamiento.

2. Una Parte no podrá, con el fin de proteger la vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra Parte.

3. Sin embargo, cualquier Parte tendrá la facultad de establecer una excepción a las disposiciones del párrafo 2:

a) En la medida en que su legislación prevea una reglamentación específica para determinadas categorías de datos de carácter personal o de ficheros automatizados de datos de carácter personal, por razón de la naturaleza de dichos datos o ficheros, a menos que la reglamentación de la otra Parte establezca una protección equivalente;

b) cuando la transmisión se lleve a cabo a partir de su territorio hacia el territorio de un Estado no contratante por intermedio del territorio de otra Parte, con el fin de evitar que dichas transmisiones tengan como resultado burlar la legislación de la Parte a que se refiere el comienzo del presente párrafo.²⁵

La legislación mexicana contiene los supuestos, y hacer mención que la palabra técnica que utiliza es la de *Transferencia*, la cual está prevista en la fracción XXXIII del

²⁵ MEXICO. Instituto Nacional de Transparencia, Acceso a la información y protección de Datos Personales. **Convenio 108 del Consejo De Europa, para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de carácter personal.** 28 de Enero de 1981. Disponible en: <http://inicio.ifai.org.mx/Estudios/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf> Acceso el 15 de agosto de 2020.



artículo 3 de la Ley General, y la define como: *Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.*

d) Protocolo Adicional al Convenio 108 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. Estrasburgo. 2001

Del Protocolo Adicional al Convenio 108, se advierte que el tema toral, es la “autoridad de control” como responsable de garantizar el cumplimiento de la regulación del derecho interno en cumplimiento al contenido del convenio.

Asimismo, el Protocolo contempla también, la regulación para los Estados u organizaciones que no sean Parte del el Convenio, pero que sin embargo hacen uso de la transferencia de datos, Estados, que deben garantizar de conformidad con el Protocolo Adicional, un nivel de protección adecuado de la transferencia de datos a juicio de la autoridad competente, de conformidad con el derecho interno de cada Estado. Lo que amplía el espectro de participación entre los Estados, y regula el ámbito de protección y participación de los flujos de datos transfronterizo.

En el caso de México la Autoridad de Control es el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales²⁶, que de conformidad con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados²⁷, es el organismo garante de la Federación en materia de protección de datos personales en posesión de los sujetos obligados como lo previene la fracción XVII del artículo 3. Cuyas facultades e integración están previstos en la misma legislación en el artículo 88 y 89 y las siguientes XXXVII fracciones. A nivel entidades federativas, el artículo 116 fracción VIII, faculta a los congresos de los estados a la creación de los organismos autónomos para garantizar el derechos de acceso a la información y protección de datos personales en posesión de los sujetos obligados, con base al artículo & de la CPEUM.²⁸

²⁶ MEXICO. Cámara de Diputados. **Ley Federal de protección de Datos Personales en Posesión de los Particulares.** 5 de julio de 2010. Artículo 38. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/ref/lfpdppp/LFPDPPP_orig_05jul10.pdf Acceso el 15 de agosto de 2020.

²⁷ Cfr. MEXICO. Cámara de Diputados. **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.** 26 de enero de 2017. Disponible en: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf> <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf>.

²⁸ MEXICO. Cámara de Diputados. **Constitución Política de los Estados Unidos Mexicanos.** 5 de febrero de 1917. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf_mov/Constitucion_Politica.pdf Acceso del 15 de agosto del 2020.



e) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

La Unión Europea, puede ser considerada como pionera de la protección jurídica digital de los datos personales, y que ante las conocidas amenazas cibernéticas que continúan en crecimiento, tuvo a bien elaborar un Reglamento General de Protección de Datos (GDPR)²⁹ de fecha de 27 de abril de 2016, en vigor el día 25 de mayo de 2018, para fortalecer lo ya existente, garantizar que los sitios web obtengan los correspondientes permisos y protejan la información que recogen de los usuarios de la Unión Europea y de todos aquellos países que ofrezcan servicios en ese mercado, actualizando sus políticas y cuidando las estrategias de privacidad.

Aun cuando dicho Reglamento forma parte del sistema europeo, no deja de ser un referente importante en el tema para analizar la tendencia de la regulación internacional, del cual invito a consultar y me limitare a reproducir algunas definiciones innovadoras de su artículo 4:

«datos genéticos»: *datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;*

«datos biométricos»: *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;*

«datos relativos a la salud»: *datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;*³⁰

²⁹ BELGICA. Diario Oficial de la Unión Europea. **Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo** de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) en vigor a partir de mayo de 2018. Disponible en: <https://www.boe.es/doue/2016/119/L00001-00088.pdf> Acceso el 15 de agosto de 2020.

³⁰ BELGICA. Diario Oficial de la Unión Europea. **Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo** de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) en vigor a partir de mayo de 2018. Disponible en: <https://www.boe.es/doue/2016/119/L00001-00088.pdf> Acceso el 15 de agosto de 2020.



4. CASO DE MÉXICO. MARCO JURIDICO Y LA IMPORTANCIA DE UN ADECUADO TRATAMIENTO DE LOS FLUJOS DE DATOS TRANSFRONTERIZO ENFOCADO A LA ADMINISTRACIÓN PÚBLICA

En México existen varios antecedentes que marcan el inicio de la regulación con transparencia con una legislación sobre el medio ambiente denominada Ley General de Protección y Equilibrio Ecológico de 1996, con posterioridad retomando la experiencia internacional se crea la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental del 11 de junio de 2002, su correspondiente reglamento en 2003³¹ Siendo los primeros esfuerzos por legislar y sumarse al concierto internacional en la materia.

En el mismo sentido, las reformas constitucionales de 2009 a los artículos 16 y 73 reafirman la protección de los datos personales, y facultan al Congreso para legislar en la materia, sin embargo, se advertían dos grandes problemas:

La legislación en materia de protección de datos personales en el sector público no garantizaba la totalidad de derechos de acceso, rectificación, cancelación y oposición, y el segundo problema estaba relacionado a la falta de normativa que aplicara a la protección de datos personales en el sector privado.

En este sentido, fue en 2010 cuando por primera vez se contó con disposiciones expresas que las empresas observarían para el tratamiento de datos personales en el sector privado, a través de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Finalmente, en 2017, se emitió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, con la cual se terminó de armonizar la normativa en la materia en México. Así, se tienen dos legislaciones específicas que dictan obligaciones, deberes, procedimientos, sanciones y recursos en la materia, tanto para el sector público como privado.³²

Hoy en México, el derecho de protección de datos personales es un derecho humano que se reconoce a nivel constitucional en el artículo 16 párrafo segundo, en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, del 26 de

³¹ Cfr. GUADARRAMA, Rabindranath. **Antecedentes de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.** Disponible en: <http://ordenjuridico.gob.mx/Congreso/pdf/39.pdf> Acceso el 15 de agosto de 2020.

³² Cfr. MENDOZA, Enriquez, OLIVIA, Andrea. **Marco jurídico de protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento.** Rev. IUS: vol. 12 no. 41 Puebla ene./jun. 2018 Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472018000100267 Acceso el 15 de agosto de 2020.



enero de 2011³³ (LGPDPSSO) para el sector público, en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares del 5 de julio de 2011³⁴, (LFPDPPP) y en el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares del 21 de diciembre de 2011³⁵ (RFPDPPP).

Sin embargo, el derecho a la protección de datos personales no puede ser comprendido al margen del derecho a la vida privada como ya ha sido ampliamente abordado y con el derecho al acceso a la información que tiene toda persona respecto a la autoridad federal, de los estados y municipal, lo que hace más interesante y complejo la correcta observancia del derecho a la protección de los datos personales de las personas por parte de la administración pública y su flujo transfronterizo.

¿Cómo considerar los derechos humanos de acceso a la información, al acceso a las tecnologías y a la transparencia en un mundo globalizado sin afectaciones a los derechos humanos como el de la privacidad, la protección de datos personales y seguridad jurídica entre otros?

Este derecho constitucional está regulado por la Constitución Política de los Estados Unidos Mexicanos en el artículo 6 A³⁶.

Es la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, reglamentaria de los artículos 6° base A y 16 segundo párrafo de la CPEUM en materia de protección de datos personales en posesión de sujetos obligados la que determina como sujetos obligados, a toda autoridad, entidad, órgano y organismo de los Poder Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos tanto del ámbito federal, estatal y municipal, incluyendo sindicatos o cualquier persona física o moral que administre recursos públicos del Estado o ejerza actos de autoridad, en el ámbito de su competencia.

Los demás supuestos deberán seguir los lineamientos previstos en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Asimismo con la Ley General en comento, resulta indispensable su conocimiento para comprender el significado y trascendencia de estos instrumentos; ¿cuál es su objeto?; ¿quiénes pueden participar?; ¿Qué principios los regulan?, y sobre todo las reglas

³³ MEXICO. Cámara de Diputados. **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados**. 26 de enero de 2017. Disponible en: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf>

³⁴ MEXICO. Cámara de Diputados. **Ley de Federal de Protección de Datos Personales en Posesión de los Particulares**. 5 de julio de 2011 Disponible en: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf> Acceso el 10 de agosto de 2020.

³⁵ MEXICO. Cámara de Diputados. **Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares**. 21 de diciembre de 2011. Disponibles en: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf Acceso el 10 de agosto de 2020.

³⁶ MEXICO. Cámara de Diputados. **Constitución Política de los Estados Unidos Mexicanos**. 5 de febrero de 1917. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf_mov/Constitucion_Politica.pdf Acceso del 15 de agosto del 2020.



internas de cada Estado para participar en el tema de flujo de datos transfronterizo, que sea seguro, confiable y con responsabilidad por parte de autoridades de control e internas que garanticen el flujo de datos con la normatividad determinada para cada país en su derecho interno, desde el marco de los derechos humanos de las personas con la debida ponderación y equilibrio entre el derecho humano a la privacidad y el derecho humano al acceso a la información, con su correspondiente protección de datos personales de los titulares de los mismos, que nuestra Constitución Política Nacional, legislación interna e Instrumentos Internacionales protegen.

La obligada atención y fortalecimiento en el tratamiento de los flujos de datos transfronterizo quedó expresada en su última reunión del 22 y 23 de mayo de 2019, en el que los Ministros que asistieron al evento, destacaron la importancia sobre la seguridad y la privacidad de datos,

...reconocieron que mejorar la seguridad, salvaguardar los datos personales, la privacidad y proteger a los consumidores, genera confianza pública en la transición digital que está en marcha....Además sostuvieron que esta confianza del público es determinante pues facilita el flujo de datos y promueve la innovación....Los miembros reconocieron que los gobiernos y otras partes interesadas incluida la industria, pueden hacer más para promover una gestión de datos responsable, efectiva y confiable, y que se esforzarán por trabajar juntos para abordar mejor estos retos.³⁷

Con la emergencia del COVID 19, México y el mundo entero emergen a una nueva era en la protección de datos personales, que han conducido a los distintos gobiernos a recurrir a tecnologías digitales para recabar, procesar y compartir datos personales para obtener respuestas eficaces frente a la pandemia, pero que sin duda, ha generado polémica en cuanto al riesgo para la privacidad de la ciudadanía en Estados donde la transparencia no es factible. Las autoridades responsables en los distintos países están adoptando un enfoque pragmático con criterios propios y emergentes apegándose lo más posible al cumplimiento legal, pero al tratarse de un tema tan sensible, sabemos que la ponderación entre el respeto a los derechos humanos a la privacidad y la protección de datos personales, la emergencia sanitaria, la formulación de políticas y decisiones públicas colocan en un estado de mayor vulneración de estos derechos humanos frente a la tecnología digital que ya opera, la tecnología 5 G, las TICs, las TACs, que a pesar de los beneficios que representan estas tecnologías y plataformas que están siendo utilizadas mayormente por el tema de la pandemia para home office, educación y ventas a distancia, reuniones con distintas plataformas de videoconferencias.

³⁷ MORAL, Yolanda. La OCDE está lista para fortalecer tributación de empresas digitales. México. **El economista**. 22 mayo de 2019. Disponible en: <https://www.economista.com.mx/economia/La-OCDE-esta-lista-para-fortalecer-tributacion-de-empresas-digitales-20190523-0078.html> Acceso el 15 de agosto de 2020.



Ahora bien, se están utilizando apps y otras plataformas y bases de datos por el tema de la pandemia, por lo que los gobiernos deben garantizar la total transparencia, rendición de cuentas así como el adecuado y oportuno ejercicio de la revocación del uso de los datos personales al fin de la crisis de pandemia.³⁸

En este tenor, en el caso de México, la Constitución Política de los Estados Unidos Mexicanos (CPEUM), reconoce los casos de excepción en el tema de protección de datos, donde está considerada la salud pública en el artículo 16 párrafo segundo.³⁹

Asimismo la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (2017), contempla en su artículo 6°, confirma la excepción por cuestiones de salud, lo que se traduce hoy, en la exposición más grande en la historia de la humanidad del derecho humano a la privacidad de las personas, pudiendo colocarse este derecho en franca sumisión ante la emergencia sanitaria por el COVID 19 que ha instado a los distintos gobiernos a utilizar y obligar en algunos países a la población a hacer uso de aplicaciones digitales y apps que acceden a datos personales, con el pretexto de prevenir y detectar probables casos de COVID en las personas.

Por su parte la Ley Federal de Protección de Datos Personales en Posesión de los Particulares de 2010 señala también en su artículo 10 casos de excepción para otorgar el consentimiento cuanto lo prevea una Ley, sean fuentes de acceso público, se vinculen a obligaciones derivadas de una relación jurídica entre titular y responsable, situación de emergencia con potencial daño, y temas vinculados a la asistencia sanitaria o por resolución de autoridad competente.⁴⁰

Por su parte, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados señala como excepciones en los artículos 6 y 7 lo siguiente:

Artículo 6. El Estado garantizará la privacidad de los individuos y deberá velar porque terceras personas no incurran en conductas que puedan afectarla arbitrariamente. El derecho a la protección de los datos personales solamente se limitará por razones de seguridad nacional, en términos de la ley en la materia, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Artículo 7. Por regla general no podrán tratarse datos personales sensibles, salvo que se cuente con el consentimiento expreso de su titular o en su defecto, se trate de los casos

³⁸ Cfr. Organización para la Cooperación el Desarrollo Económicos. Medidas políticas clave de la OCDE ante el coronavirus (COVID-19) Garantizar la privacidad de datos mientras luchamos contra el COVID-19. 14 de abril 2020. Disponible en: <http://www.oecd.org/coronavirus/policy-responses/garantizar-la-privacidad-de-datos-mientras-luchamos-contra-el-covid-19-49dc1537/> Acceso del 15 de agosto de 2020

³⁹ Cfr. MEXICO. Cámara de Diputados. **Constitución Política de los Estados Unidos Mexicanos**. 5 de febrero de 1917. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf_mov/Constitucion_Politica.pdf Acceso del 15 de agosto del 2020.

⁴⁰ MEXICO. Cámara de Diputados. **Ley Federal de protección de Datos Personales en Posesión de los Particulares**. 5 de julio de 2010. Artículo 38. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/ref/lfpdppp/LFPDPPP_orig_05jul10.pdf Acceso el 15 de agosto de 2020.



*establecidos en el artículo 22 de esta Ley. En el tratamiento de datos personales de menores de edad se deberá privilegiar el interés superior de la niña, el niño y el adolescente, en términos de las disposiciones legales aplicables.*⁴¹

La LFPDPPP define como datos sensibles en su artículo 3º inciso VI como sigue:

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

Asimismo, en el artículo 9º precisa que:

Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.

Y en el artículo 10º, precisa cuando no es necesario el consentimiento para el tratamiento de datos personales, porque de no tener un trato adecuado de los mismos, sin duda se estarían violentando los derechos humanos del o la titular de los datos, que son defendibles por la vía jurisdiccional o no jurisdiccional a través de los organismos de derechos humanos.

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

- I - Esté previsto en una Ley;*
- II - Los datos figuren en fuentes de acceso público;*
- III - Los datos personales se sometan a un procedimiento previo de disociación;*
- IV - Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;*
- V - Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;*
- VI - Sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios,*

⁴¹ MEXICO. Cámara de Diputados. **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados**. 26 de enero de 2017. Disponible en: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf> <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf>.



mientras el titular no esté en condiciones de otorgar el consentimiento, en los términos que establece la Ley General de Salud y demás disposiciones jurídicas aplicables y que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente, o

VII - Se dicte resolución de autoridad competente.”⁴²

5. LOS POSIBLES RIESGOS ANTE LA INNOVACIÓN TECNOLÓGICA MEDIANTE EL ANÁLISIS DE LA ÉTICA EN EL USO DE LAS NUEVAS TECNOLOGÍAS

Cabe preguntarse, ¿Qué papel juega la ética frente a los riesgos de las nuevas tecnologías?

“¿Que es la ética digital? No es una palabra que frecuentas en cualquier diccionario, por lo tanto, está definida por expertos como “el impacto de las tecnologías de información y comunicación digitales (TIC) en nuestras sociedades y ambiente en general”⁴³

La ética como la moral y los valores humanos, están íntimamente vinculados y tienen como fin común el bien vivir de los seres humanos, siendo los valores de la ética fundamento y esencia de los derechos humanos universales, que hoy representan el soporte de todo Estado democrático de derecho.

Es por ello que la ética representa hoy día, una mancuerna insoslayable del quehacer público y privado, para que guíe y oriente la conducta humana, objeto del derecho, es por ello que la ética debe estar en el centro, al igual que los derechos humanos para la construcción de la normatividad jurídica.

La era digital y tecnológica que vivimos hoy en día, ponen en riesgo el derecho a la vida privada y la protección de los datos personales ante la falta de regulación y límites en la materia, por lo que emergen iniciativas como la de la Unión Europea en donde se están haciendo grandes esfuerzos para regular la materia, tanto internacional como internamente en cada país.

Por lo que es importante hacer un llamado significativo para enseñar la importancia de la reconstrucción de valores humanos, valores sociales, valores nacionales, traducidos en la ética profesional, para que con la transfronterización o transferencia de datos personales e información, se cuente con un código ético, que limite los riesgos de vulneración de derechos humanos vinculados a la privacidad, al acceso a la información y sin duda a la dignidad de las personas.

⁴² MEXICO. Cámara de Diputados. **Ley Federal de protección de Datos Personales en Posesión de los Particulares**. 5 de julio de 2010. Artículo 38. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/ref/lfpdppp/LFPDPPP_orig_05jul10.pdf Acceso el 15 de agosto de 2020.

⁴³ LLAVES, Ricardo. **La ética digital y la privacidad de nuestros datos**. 18 de febrero 2019 Disponible en: <https://ricardollarves.com.ve/la-etica-digital-y-la-privacidad-de-nuestros-datos/> Acceso 15 de agosto de 2020.



El desconocimiento, minimización e ineficacia de los derechos mencionados, pondrá en grave riesgo a cualquier sociedad y a sus instituciones, en un mundo globalizado como el que ahora conocemos, que evoluciona cada vez más hacia la digitalización de datos e información; su resguardo y regulación no puede soslayar los valores humanos ni los derechos humanos, como bien lo señalan las Directrices de la OCDE, el convenio 108 de Estrasburgo, su Protocolo adicional, y la Reglamentación de la Unión Europea para la protección de de datos personarles de 2018.

Cuando se habla de crisis de valores éticos de la juventud se tendría que recordar esto. Lo que sucede muchas veces es que los jóvenes tienen una profunda ignorancia respecto a cada uno de los valores, y esto se agrava cuando no ven vividos esos valores en sus padres y maestros, con lo cual no pueden contemplarlos.⁴⁴

La etiqueta digital es esencial para fortalecer su reputación (como ente público o privado), retener a sus clientes y comportarse éticamente en el mundo digital.

La comprensión de la **ética y la privacidad** puede parecer simple al principio, pero cuando empiezas a sumergirte, descubres que encontrar el equilibrio entre ser solidario e intrusivo es difícil.⁴⁵

6. CONCLUSIONES

Hoy México cuenta con un marco jurídico para la protección de datos personales tanto públicos como privados garantizados en la Constitución Federal, y a partir de la firma de adhesión al Convenio 108 y a su Protocolo Adicional, con fundamento en el artículo 1 de la CPEUM, se adquieren compromisos internacionales que facilitarán el flujo transfronterizo de datos, su tratamiento e información en beneficio de los Estados y de los derechos de las personas titulares de la información, pero también adquiere obligaciones y responsabilidades por un mal tratamiento de los mismos desde la técnica jurisdiccional como desde la perspectiva de los derechos humanos.

En el ámbito de la administración pública, después de haber comprendido la génesis de su observancia a nivel internacional, el adentrarse a la previsión de la CPEUM, a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, reglamentaria de los artículos 6° base A y 16 segundo párrafo de la CPEUM en materia de protección de datos personales en posesión de sujetos obligados se tiene una mayor claridad de esta temática imprescindible en el tratamiento de los datos personales en el poder público donde México es un referente importante.

⁴⁴ 2. CASTILLO, Genaro. **La educación en los Valores. Ética y educación en valores.** Disponible en: http://www.biblioteca.udep.edu.pe/BibVirUDEP/libro/pdf/1_33_70_22_207.pdf Acceso el 15 de agosto de 2020.

⁴⁵ Cfr. LLAVES, Ricardo. **La ética digital y la privacidad de nuestros datos.** 18 de febrero 2019. Disponible en: <https://ricardollarves.com.ve/la-etica-digital-y-la-privacidad-de-nuestros-datos/> Acceso 15 de agosto de 2020



A pesar de que el marco jurídico en materia de protección de datos personales en posesión de las autoridades y las empresas de servicio establecidas en México, es acorde a los estándares internacionales y proporcionan garantías para la efectiva tutela de este derecho, el cumplimiento de las disposiciones legales enfrenta grandes desafíos aun, desde la falta de ética en dicho tratamiento, hasta el desconocimiento de los contenidos legales para el tratamiento de la información, la falta de sensibilización respecto a las repercusiones del mal uso de la información y el desconocimiento de los mecanismos legales para exigir este derecho.

La ética es un elemento crucial para la seguridad y el éxito de la regulación del acceso a la tecnología de la información y las comunicaciones, que impidan confundir los valores que existen y el uso ético de estas herramientas, lo cual es indispensable para la seguridad de las TICs, de tal manera que se evite comprometer la protección de los datos personales. La ética debe ser el tamiz para la construcción jurídica de toda norma jurídica. La ética y el respeto a los derechos humanos son el crisol para una sociedad democrática y de derecho.

REFERENCIAS

BELGICA. Diario Oficial de la Unión Europea. **Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo**, 27 de abril de 2016. Disponible en: <https://www.boe.es/doue/2016/119/L00001-00088.pdf> Acceso el 15 de agosto de 2020.

CASTILLO, Genaro. **La educación en los Valores. Ética y educación en valores**. Disponible en: http://www.biblioteca.udep.edu.pe/BibVirUDEP/libro/pdf/1_33_70_22_207.pdf Acceso el 15 de agosto de 2020.

FRANCIA. Organización para la Cooperación Económica Europea. **Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales**. 23 de septiembre de 1980. Disponible en: http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf Acceso el 15 de agosto de 2020.

FRANCIA. Consejo de Europa. **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**. 8 de noviembre de 2001. Disponible en: <https://rm.coe.int/16806c1abe> Acceso el 15 de agosto de 2020.

GUADARRAMA, Rabindranath. **Antecedentes de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental**. Disponible en: <http://ordenjuridico.gob.mx/Congreso/pdf/39.pdf> Acceso el 15 de agosto de 2020.

LLAVES, Ricardo. **La ética digital y la privacidad de nuestros datos**. 18 de febrero 2019. Disponible en: <https://ricardollarves.com.ve/la-etica-digital-y-la-privacidad-de-nuestros-datos/> Acceso 15 de agosto de 2020



LUXEMBURGO. Parlamento Europeo. **Directiva 95/46/CE del Parlamento Europeo y del Consejo**, 24 de octubre de 1995. Disponible en: EUR-Lex - 31995L0046 - EN - EUR-Lex (europa.eu) Acceso 10 de agosto de 2020.

MENDOZA, Enriquez, OLIVIA, Andrea. **Marco jurídico de protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento**. Rev. IUS: vol. 12 no. 41 Puebla ene/jun. 2018 Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472018000100267 Acceso el 15 de agosto de 2020.

MEXICO. Cámara de Diputados. **Constitución Política de los Estados Unidos Mexicanos**. 5 de febrero de 1917. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf_mov/Constitucion_Politica.pdf Acceso del 15 de agosto del 2020.

MEXICO. Cámara de Diputados. **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados**. 26 de enero de 2017. Disponible en: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf>.

MEXICO. COMISIÓN NACIONAL DE LOS DERECHOS HUMANOS. **Que son los derechos humanos**. Disponible en: http://www.cndh.org.mx/Que_son_derechos_humanos Acceso el 15 de agosto del 2020.

MÉXICO. Diario Oficial de la Federación. **Decreto Promulgatorio del Convenio 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 mil novecientos ochenta y uno. 28 de septiembre de 2018. Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5539473&fecha=28/09/2018 Acceso el 15 de agosto de 2020.

MEXICO. Instituto Nacional de Transparencia, Acceso a la información y protección de Datos Personales. **Convenio 108 del Consejo De Europa, para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de carácter personal**. 28 de Enero de 1981. Disponible en: <http://inicio.ifai.org.mx/Estudios/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf> Acceso el 15 de agosto de 2020.

MOLET, Jorge. El Economista. . **Adopción de México del Convenio 108 del Consejo de Europa, protección y flujo internacional de datos**. 20 de junio de 2018. Disponible en: <https://www.eleconomista.com.mx/opinion/Adopcion-de-Mexico-del-Convenio-108-del-Consejo-de-Europa-proteccion-y-flujo-internacional-de-datos-20180620-0098.html> Acceso el 15 de agosto de 2020.

MORAL, Yolanda. La OCDE está lista para fortalecer tributación de empresas digitales. México. **El economista**. 22 mayo de 2019. Disponible en : <https://www.eleconomista.com.mx/economia/La-OCDE-esta-lista-para-fortalecer-tributacion-de-empresas-digitales-20190523-0078.html>. Acceso el 15 de agosto de 2020.

MORALES, Yolanda. La OCDE está lista para fortalecer tributación de empresas digitales. **El economista**. 23 de mayo de 2019. Disponible en: <https://www.eleconomista.com.mx/economia/La-OCDE-esta-lista-para-fortalecer-tributacion-de-empresas-digitales-20190523-0078.html>. Acceso el 15 de agosto de 2020.



OCDE. **Directrices de la OCDE que regulan la protección de la privacidad y el Flujo transfronterizo de datos personales.** 23 de septiembre de 1980. Disponible en: http://www.oas.org/es/sla/ddi/docs/directrices_ocde_privacidad.pdf Acceso el 15 de agosto de 2020.

OCDE. **Directrices de la OCDE que regulan la protección de la privacidad y el Flujo transfronterizo de datos personales.** 23 de septiembre de 1980. Disponible en: http://www.oas.org/es/sla/ddi/docs/directrices_ocde_privacidad.pdf Acceso el 15 de agosto de 2020.