Exposición del Programa de Trabajo como Comisionado del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

2020-2027

Mtro. Javier Martínez Cruz

Hacia el Futuro. Misión y Visión

I. Misión. Garantizar en su totalidad la igualdad de condiciones para que cualquier persona conozca, acceda y ejercite los derechos de Acceso a la Información y a la Protección de Datos Personales, observando los principios constitucionales y una interpretación progresiva y garantista de estos derechos humanos previstos en la Ley Fundamental y en los tratados internacionales de los que México es parte.

II. Visión. A través de las atribuciones y de acuerdo con la Constitución Política de los Estados Unidos Mexicanos, consolidar el Acceso a la Información Pública y la protección de los datos personales, y el pleno ejercicio de los derechos de acceso, rectificación, cancelación, oposición y la portabilidad de datos personales en la Federación, a través de la implementación, promoción y difusión de una Cultura en estas materias.

Lo anterior, sin dejar a un lado la necesidad de abordar, de una manera integral, eficiente y comprometida, la relación de estos Derechos y la sociedad, así como los intereses nacionales en temas cruciales del Derecho y del desarrollo social, económico y político.

III Introducción

El acceso a la Información Pública y la Protección de Datos personales en posesión de los Sujetos Obligados, son dos derechos humanos previstos en nuestra Constitución General, que deben ser garantizados de manera eficiente y eficaz por los Órganos garantes respectivos, tanto en el ámbito Federal como en cada entidad federativa, prerrogativas cuya progresión legislativa se ha intensificado a partir del año 2011 y hasta 2016, otorgando la facultad al organismo garante, INAI, de coordinar sus acciones con la Auditoría Superior de la Federación, con la entidad especializada en materia de archivos y con el organismo encargado de regular la captación, procesamiento y publicación de la información estadística y geográfica, así como con los organismos garantes de las entidades federativas, con el objeto de fortalecer la rendición de cuentas del Estado Mexicano.

En este sentido, el Plan de Trabajo que me propongo desarrollar contiene acciones concretas y líneas de acción que se seguirán en cinco pilares fundamentales, mismos que considero de suma importancia su ejecución y, que en conjunto, coadyuvarán al pleno ejercicio y difusión de la cultura del Acceso a la Información, la transparencia y rendición de cuentas, protección de datos personales, así como a la promoción del Sistema Nacional de Transparencia y la adopción de valores democráticos en la Sociedad en general.

Así, para consolidar el Sistema Nacional Anticorrupción a través de la Transparencia y Acceso a la Información Pública he decidido que resulta de vital importancia desde el Órgano Garante Nacional promover la participación de la sociedad en el ejercicio de este derecho, con el cual se permite el fortalecimiento de los derechos humanos, así

como conocer la gestión gubernamental y evaluar a los servidores públicos en el ejercicio de sus funciones; así mismo, es necesario que la transparencia se convierta en un elemento presente en la función pública, para abatir la impunidad y combatir la corrupción.

De forma muy especial, a través del INAI crear marcos de colaboración con la Secretaría de Educación Pública (SEP), con universidades públicas y privadas a fin de que, temas de transparencia y combate a la corrupción se vean incluidos en la reformulación de **contenidos de las materias de civismo y ética**, lo cual tendría un impacto positivo a largo plazo en toda nuestra sociedad en virtud de que en nuestros niños y jóvenes se estarían permeando valores tendientes a combatir la corrupción en todas sus formas.

Sin olvidar los ajustes razonables, adecuados, idóneos y suficientes que faciliten que **grupos vulnerables** —como las personas con discapacidad o pertenecientes a comunidades originarias— puedan hacer solicitudes de información para ejercitar estos derechos.

Por otro lado, hoy en día realmente la población se preocupa por proteger sus datos personales tomando en cuenta que vivimos en un mundo tecnológico y nuestros datos en el ámbito digital quedan contenidos en múltiples sitios. Un tema pendiente en la agenda de la protección de datos personales es sin lugar a dudas la prevención, disuasión y la sanción de todo acto de violencia digital y sexual, en consideración de que los sobrevivientes de **violencia digital** enfrentan violaciones a sus derechos humanos; así como al abandono del espacio digital, lo que afecta sus entornos *offline* como escuela, trabajo, familia y relaciones públicas.

Por ello, que en el segundo pilar se contienen acciones tendientes a la protección de datos personales en contextos digitales con miras al respeto a la dignidad humana. de

forma muy especial, la importancia de tipificar la violencia ejercida a través de las tecnologías de la información y la comunicación, sobre todo al sector femenino, a fin de brindar medidas que garanticen los derechos de las y los usuarios de Internet en todo el territorio nacional, como lo propone la conocida “Ley Olimpia”.

Además, dentro de este pilar se toman en cuenta, sentar bases en la protección de los datos concernientes a las personas fallecidas donde se abre una fuente de reflexión, ya que involucra el debate de aspectos tan relevantes como la acreditación de la personalidad jurídica, el interés jurídico y el interés legítimo, en la interpretación de estas figuras, que resultan novedosas en este ámbito, deben analizarse los derechos en colisión, con el objetivo de ponderar cuáles prevalecen sobre los demás, tomando en cuenta los conceptos relacionados con el patrimonio moral de las personas.

Otro aspecto considerado, es la adhesión de México al Convenio 108 del Consejo de Europa en virtud de que este instrumento involucra numerosos retos que a la fecha no han sido atendidos; en este sentido, en el tercer pilar he decidido proponer acciones para desarrollar nuevas políticas en la materia, con el fin del alcanzar los estándares marcados por el convenio.

Las acciones que se proponen en este apartado son una oportunidad para el país, ya que podríamos aprovechar nuestra normatividad para decirle a Europa que somos un país considerado de puerto seguro para el flujo transfronterizo y establecer lazos de coordinación económica para hacer frente al difícil contexto económico global.

Finalmente, para el fortalecimiento y consolidación del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos, he considerado en el cuarto pilar la implementación de acciones tendientes a garantizar de manera efectiva la ejecución del derecho a la portabilidad de los datos personales, lo cual significa numerosos beneficios para la ciudadanía, ya que los propios titulares pueden obtener

la información que han entregado a distintas instituciones y realizar los trámites que deseen, sin necesidad de que terceras personas accedan a ella.

Así, la implementación de acciones que faciliten la portabilidad de los datos personales genera un impacto positivo, incluso, en el bolsillo de sus titulares, pues ya no deben desplazarse de una institución a otra para transferir su info rmación. Asimismo, al reducir la interacción directa entre los ciudadanos y los funcionarios, ayuda a inhibir los actos de corrupción y a potenciar la transparencia.

Eje temático.

Transparencia y acceso a la información pública para consolidar el Sistema Nacional Anticorrupción (el poder de la triada.)

Justificación.

La corrupción constituye una incuestionable transgresión y flagelación al patrimonio económico de cualquier país, este fenómeno social, cuyo origen es multifactorial repercute negativamente en elevados costos económicos que impiden el desarrollo social, político y económico de cualquier sociedad.

La corrupción en México, es un problema, que se ha engendrado en las instituciones de la administración pública de manera desproporcionada durante los últimos años, el amplio consenso que existe entre los miembros de las instituciones públicas sobre la corrupción han deteriorado la estructura institucional de manera considerable.

Ahora bien, esta conducta, que ha sido asimilada y normalizada por parte de los servidores públicos en los tres órdenes de gobierno tanto Federal, Estatal y Municipal,

ha requerido de la adopción de políticas públicas, en las que instituciones deberán trabajar en forma conjunta y coordinada para a frenar este mal que tanto aqueja a México.

En una aproximación inicial al concepto de corrupción, la podemos encontrar en la Convención Interamericana Contra la Corrupción la cual señala que la corrupción es "todo requerimiento o aceptación, directa o indirectamente, por un funcionario público o una persona que ejerza funciones públicas, de cualquier objeto de valor pecuniario u otros beneficios como dádivas, favores, promesas o ventajas para si mismo o para otra persona o entidad a cambio de la realización u omisión de cualquier acto en el ejercicio de sus funciones públicas" (OEA, 2019).

En esta misma línea, el Programa Nacional de Rendición de Cuentas, Transparencia y Combate a la Corrupción del Gobierno Federal señala que la Corrupción es "toda conducta que se desvía de la función pública reglamentada debido a una consideración de índole privada o para obtener beneficios pecuniarios o de rango; o la violación de reglas por consideraciones de carácter privado. Se refiere a la ejecución de acciones que contradicen el ordenamiento legal del Estado y que se desvían de los criterios normativos establecidos." (PNRCTCC 2008-2012).

En este sentido, se puede entender que los actos de corrupción menoscaba el ejercicio de la función pública, dando origen a una problemática compleja que distorsiona la función de los servidores públicos. De esta forma estas conductas corruptas fragmentan el sistema normativo y afectan directamente a la sociedad.

Instrumentos internacionales anticorrupción y el Estado Mexicano.

En México, el combate a la corrupción en los últimos años ha sido una cuestión que ha requerido la suscripción y ratificación de diversos instrumentos internacionales para lograr su erradicación como es la **Convención Interamericana contra la Corrupción,**

la cual fue aprobada en 1996 y ratificada un año después en 1997, la cual tiene como propósito promover y fortalecer el desarrollo, por cada uno de los Estados Partes, de los mecanismos necesarios para prevenir, detectar, sancionar y erradicar la corrupción (OEA, 2019).

Otro instrumento de cooperación internacional del cual México forma parte es la Convención de las Naciones Unidas Contra la Corrupción celebrará en Mérida (México) del 9 al 11 de diciembre de 2003, la cual tiene por finalidad Promover y fortalecer las medidas para prevenir y combatir más eficaz y eficientemente la corrupción; así como facilitar y apoyar la cooperación internacional y la asistencia técnica en la prevención y la lucha contra la corrupción. (CNUCC, 2019)

Por último la Convención para Combatir el Cohecho de Servidores Públicos Extranjeros en transacciones comerciales internacionales, la cual entre sus principales objetivos que persigue es el establecimiento de medidas eficaces para disuadir, prevenir y combatir el cohecho de servidores públicos extranjeros en relación con las transacciones comerciales internacionales.

Costo de la corrupción en México

El costo de la corrupción en México, según el Banco de México la corrupción en el país representa cerca del 10% del PIB. De acuerdo a datos del INEGI la corrupción alcanzaría 347 mil millones de pesos que equivaldrían aproximadamente el 2% del PIB (2013). Esta cifra es similar a la arrojada por “México ¿Cómo Vamos?” que la sitúa en 342 mil millones de pesos al año. El Banco Mundial estima que la corrupción cuesta a México el equivalente a 9% de su PIB y 80% de la recaudación de impuestos federales. Forbes coincide con el 9% (2014) y el CEESP la sitúa en 10% (2015). (IMCO, 2015: 42)

Entonces, a partir del estudio y de la información antes mencionada por las diferentes instituciones, el Producto Interno Bruto asciende a un total de 1, 174, 948,000 y a

corrupción equivale al 10% del PIB que según el Banco de México representa 117, 494 millones de pesos. Por lo cual si lo comparamos con los recursos asignados al presupuesto de egresos para el Estado de México en 2016 el cual asciende a 221,285,729,374[1] esto equivaldría a 117, 494 millones de pesos que representan un equivalente del 53% de este presupuesto.

Programas y Mecanismos Anticorrupción en los últimos años

Antecedentes

La magnitud e importancia del fenómeno de la corrupción como un asunto de política pública ha llevado a la creación de diversos instrumentos y órganos encargados de realizar la auditoría gubernamental y combatir a la corrupción en el país, desde la creación de la Secretaría de la Contraloría General de la Federación en 1982, la Secretaría de la Función Pública SFP en 2003 por mencionar algunos (RAMOS, 2017:8).

Reforma 2014 en materia de transparencia

A partir de mes de febrero de 2014 se publicó en el Diario Oficial de la Federación, el Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos en Materia de Transparencia, la reforma propone construir un Sistema Nacional de Transparencia (SNT) para la coordinación de los órganos garantes locales con el Instituto Nacional de Acceso a la Información (INAI), el Archivo General de la Nación (AGN), la Auditoria Superior de la Federación (ASF) y el INEGI.(DOF, 2014)

[1]Información del presupuesto fue tomado de la página electrónica del Gobierno del Estado de México, fecha de emisión 29/01/2016, link de consulta http://contabilidad.edomex.gob.mx/sites/contabilidad.edomex.gob.mx/files/files/finanzas/2016/Difusi%C3%B3n%20a%20la%20ciudadan%C3%ADa%20de%20la%20LI%20y%20PE-16.pdf

Uno de los principales objetivos que persigue la reforma, es que la sociedad podrá conocer toda la información en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal.

Ahora bien, el motivo de que en esta reforma se incorporaran nuevos sujetos obligados radica principalmente en el problema de la corrupción que actualmente enfrenta el estado mexicano, derivado del manejo de los recursos presupuestales, razón por la cual se incluye a sujetos que tengan una relación directa con el ejercicio de recursos que reciban del estado.

Por lo que, la rendición de cuentas se hará según mandata el artículo 134, de la Constitución Política de los Estado Unidos Mexicanos el cual especifica que Los recursos económicos de que dispongan la Federación, las entidades federativas, los Municipios y las alcandías de la Ciudad de México, deberán de administrarse de acuerdo a los principios de Eficiencia, Eficacia, Economía, Transparencia y Honradez (CPEUM, 2019).

Reforma 2015 Creación del Sistema Nacional Anticorrupción (SNA.).

Sin embargo, uno de los cambios más significativos en este tema se da a partir de la reforma de 2015, con la creación del Sistema Nacional Anticorrupción (SNA). De acuerdo con lo previsto en el artículo 113 Constitucional, este Sistema tiene como objetivo la coordinación de las autoridades de los tres ámbitos de gobierno en materia de prevención, detección y sanción de responsabilidades administrativas y hechos de corrupción, así como la fiscalización y control de recursos públicos (CPEUM, 2019).

En este contexto, el 18 de julio de 2016, se expide **Ley General del Sistema Nacional Anticorrupción,** la cual se constituye como el instrumento operativo de las nuevas normas de responsabilidades que requieren ser diseñadas bajo nuevas premisas de denuncia, investigación, sanción, corrección y resarcimiento del daño.(DOF, 2016)

Por ello, el **Sistema Nacional Anticorrupción,** se integra por instancias competentes y afines, cuyo objeto es coordinar sus respectivos esfuerzos a fin de implementar políticas transversales en materia de prevención, control y sanción de la corrupción. (Senado de la República, 2015).

Etapas de sistema de corrupción

El poder de la triada (Prevención, Disuasión, Sanción)

Prevención

Para llevar a cabo su máximo potencial de estas reformas, tal como está previsto en la Política Nacional Anticorrupción las acciones deben estar encaminadas en un esfuerzo continuo y articulado por el Sistema Nacional de Transparencia, Sistema Nacional de Fiscalización y el Sistema Nacional Anticorrupción. En este sentido, resulta indispensable poner especial atención en el Sistema Nacional de Transparencia ya que como etapa preventiva cumple un papel vital pues constituye la forma de participación activa de la sociedad, es la oportunidad de que el ciudadano se constituya en el fiscalizador activo de los recursos públicos, y de esta forma inhibir actos de corrupción. En este sentido, se fortalece una sociedad transparente que tiene como objetivo desarrollo económico de nuestro país.

Disuasión

Ahora bien, si la etapa preventiva no funciona corresponde a la etapa de disuasión en esta etapa los órganos de fiscalización se ocupa de la implementación de acciones que tiene como objetivo contrarrestar estas conductas corruptas.

Sanción

Por último, si ninguna de las etapas anteriores funciona, corresponde a los organismos como el Poder Judicial penalizar los actos de corrupción.

Estrategia:

El trabajo coordinado del Sistema Nacional de Transparencia, el Sistema Nacional de Fiscalización y el Sistema Nacional Anticorrupción, haciendo efectivas las etapas que deben cumplir cada uno de estos, como lo son: Prevención, disuasión y Sanción

Líneas de acción:

- Fortalecer la confianza entre los ciudadanos a través de la promoción de la transparencia y acceso a la información pública.
- Vincular el sistema Nacional de Transparencia en el control, vigilancia y sanción a los actos de corrupción.
- Proponer la creación de una base de datos que contenga los diferentes servicios que pueden brindar las autoridades a los ciudadanos a fin de fomentar la transparencia y rendición de cuentas.
- Crear herramientas innovadoras que promuevan intereses cotidianos en los ciudadanos, respecto a las acciones de los servidores públicos.
- Implementar acciones que permitan a los ciudadanos confrontarlos con

situaciones reales, que los lleven a reconocerse como factor indispensable en la lucha contra la corrupción.

- Establecer procesos que evalúen el desarrollo de prácticas transparentes en el ejercicio de los funcionarios.
- Promover la realización de campañas de sensibilización entre los servidores públicos en materia de transparencia y acceso a la información pública.

Eje temático.

Protección de datos en el contexto de los derechos digitales con respeto a la dignidad humana (personas fallecidas, Ley Olimpia.)

Justificación

Derecho a la intimidad post-mortem y la libertad de expresión

En días recientes, llamó la atención de la sociedad mexicana la irresponsable divulgación de las imágenes de la escena del feminicidio de **Ingrid Escamilla** en algunos diarios de nota roja. A raíz de estos hechos, provoco el descontento de ciertos sectores de la sociedad en su mayoría mujeres, quienes en el hartazgo social realizaron distintas marchas para manifestar su rechazo a la publicación y exigir al medio de comunicación una disculpa.

Hoy en día, muchos son los ejemplos en México en el que los medios de comunicación difunden este tipo de imágenes sensacionalistas que alientan el morbo, desensibilizan

a la sociedad y normalizan así la violencia de género, sin que haya un reproche social o legal que límite dichos contenidos excesivos de violencia y carentes de empatía.

Es evidente que la publicación indiscriminada de este tipo de imágenes, bajo el amparo de la libertad de expresión, atenta contra el derecho a la protección de datos personales y la intimidad del que goza todo ser humano. Si bien es cierto, que la muerte del sujeto de derecho extingue los derechos de la personalidad, no obstante, la memoria de aquel constituye una prolongación de esta última que debe también ser tutelada por el derecho (Muñozcano, 2010, p. 61).

Estas limitantes y el reconocimiento de estos derechos han tenido buena acogida en otros países, por ejemplo, el Tribunal Constitucional Español, señala que la titularidad de los derechos fundamentales se extingue en principio con la muerte de la persona y, de acuerdo con ello una vez que ha muerto el titular del derecho lesionado, desaparece el medio de defensa. No obstante, esto no impide que algunos derechos señaladamente los derechos al honor, a la intimidad y a la propia imagen puedan tener cierta eficacia post mortem, y en esos casos serán los familiares los que podrán acudir al medio de defensa (STC, 190/1996).

De manera similar el Instituto de Acceso a la Información Pública del Salvador, señala respecto a este tema que, una persona fallecida no es titular de datos personales, por no ser una persona natural, su honra, sin embargo, se proyecta como un derecho propio de sus familiares toda vez que su memoria constituye una prolongación de dicha personalidad (IAIP, NUE 56-A-2015).

En este sentido, si bien es cierto que el derecho a la libertad de expresión permite recibir, buscar y difundir información, sin embargo cuando se traten imágenes o cualquier otro dato personal que puedan afectar la intimidad de las víctimas o sus

familiares, este ejercicio deberá realizarse de una forma más restrictiva, menos abierta y lesiva de manera que puedan coexistir ambos derechos.

Por último, es importante resaltar sin duda alguna que, las imágenes publicadas en estos diarios son el vivo reflejo de las deficiencias institucionales estatales y la actividad criminal omnipresente en México. Sin embargo, este fenómeno no puede ser visto como un centro de comercio, en el que a las imágenes llenas de violencia explícita se les atribuye un valor, sin importar la vulneración a la intimidad de las víctimas y el daño que pueden causar a sus familiares.

En una sociedad globalizada en donde las tecnologías posibilitan el intercambio y flujo masivo de información de los particulares, la protección de los datos personales es un tema que requiere de atención inmediata por parte del Estado para salvaguardar este Derecho Humano.

Actualmente, la vida no se entendería por completo sin el uso cotidiano de aplicaciones tecnológicas, plataformas digitales y redes sociales a través del internet. Esta herramienta, por una parte facilita la vida individual y colectiva, y por la otra vulnera la información de los usuarios en el uso no autorizado, indebido y/o ilegal de sus datos.

De acuerdo a la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2019[2], en nuestro país hay 80.6 millones de usuarios de internet, que representan el 70.1% de la población de seis años o más. Esta cifra revela un aumento de 4.3 puntos porcentuales respecto de la registrada en 2018 (65.8%) y de 12.7 puntos porcentuales respecto a 2015 (57.4 por ciento). Entre 2017 y

[2] Encuesta realizada por el Instituto Nacional de Estadística y Geografía (INEGI), en colaboración con la Secretaría de Comunicaciones y Transportes (SCT) y el Instituto Federal de Telecomunicaciones (IFT). https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2020/OtrTemEcon/ENDUTIH_2019.pdf (consultada el 24 de marzo de 2020)

2019, los usuarios en la zona urbana pasaron de 71.2% a 76.6%, mientras que en la zona rural el incremento fue de 39.2% a 47.7% de usuarios de 6 años o más.

Si bien es cierto que las Tecnologías de la Información y de Comunicación (TIC´s) ofrecen nuevas oportunidades y potentes herramientas para que las personas, sus comunidades y sus organizaciones puedan mejorar notablemente la calidad de sus vidas y promover un desarrollo sostenible, también vulneran los derechos humanos[3].

Los derechos digitales por un lado deben promover y proteger los derechos y humanos, y por el otro, salvaguardar los derechos inherentes a la persona, como son a la protección de los datos personales, a la libertad de expresión y al honor. El deber del Estado frente al derecho de los gobernados a decidir qué aspectos de su vida da o no a conocer, o cuáles reserva para sí mismo y cuáles comparte con la sociedad, conlleva la obligación estatal de dejarlos exentos e inmunes a invasiones agresivas o arbitrarias por parte de terceros o de la autoridad pública.

Esta función debe acentuarse ante posibles delitos como son ciberviolencia de género, el *ciberbullying*, el *grooming* o ciberacoso sexual, el *sexting*, la sextorsión, el robo de identidad, y la pornovenganza o porno vengativo.

Ante estas situaciones, el Estado debe establecer, implementar y hacer cumplir marcos legales integrales para proteger la privacidad y los datos personales de los ciudadanos, que deben estar en consonancia con las normas internacionales de derechos humanos

[3] carta de derechos humanos y principios para internet. ONU. 2015. http://derechoseninternet.com/docs/IRPC_Carta_Derechos_Humanos_Internet.pdf (fecha de consulta 24 de marzo de 2020)

e incluir la protección contra violaciones de privacidad por parte del Estado y de las empresas privadas.

Datos Personales de Personas fallecidas

Otro aspecto importante que no se debe perder de vista, es la protección de datos personales de las ***personas fallecidas***, aspecto que se encuentra relacionado con el denominado "**interés legítimo**", que en términos de Ferrer Mac-Gregor, es *"una situación jurídica activa que se ostenta por relación a la actuación de un tercero y que no supone, a diferencia del derecho subjetivo, una obligación correlativa de dar, hacer o no hacer, exigible de otra persona, pero sí comporta la facultad del interesado de exigir el respeto del ordenamiento jurídico y, en su caso, de exigir una reparación de los perjuicios antijurídicos que de esa actuación le deriven.*[4]

Concepto que ha evolucionado a partir de las reformas de nuestra Constitución General a partir del año 2011 y que se observa en el contenido de la fracción I del artículo 107 Constitucional en materia de Amparo, así como en la fracción I del artículo 5 de la Ley de Amparo.

Así, en materia de Protección de Datos Personales, específicamente de las personas fallecidas, Muñoz Eternod menciona que la muerte del sujeto de derecho extingue los derechos de la personalidad, la memoria de aquél constituye una prolongación de esta última que debe también ser tutelada por el Derecho.[5]

[4] Citado en: Diccionario de Derecho Procesal Constitucional y Convencional 2014 Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM. Disponible en https://archivos.juridicas.unam.mx/www/bjv/libros/8/3683/13.pdf. Fecha de consulta 10 mayo de 2019

[5] Muñozcano Eternod A "El Derecho a la Intimidad frente al Derecho a la Información" ed. Porrúa México. 2010

No obstante, ello no impide que algunos derechos intrínsecos como el derecho al honor, a la intimidad, la propia imagen; en materia de salud y expediente clínico; tengan cierta eficiencia ***post mortem***, que ante dicha situación se concreta dicho interés legítimo a favor de los familiares de las personas fallecidas, como pueden ser el cónyuge o concubino supérstite, los parientes en línea recta ascendente y descendente sin limitación de grado, y en línea transversal hasta el segundo grado y en caso de que no existan las personas referidas, tendrán la potestad de ejercer los derechos ARCO, los Parientes en línea transversal hasta el cuarto grado, previa acreditación de su identidad mediante identificación oficial, tener interés legítimo o jurídico a través del documento respectivo, así como el acta de defunción del fallecido, como actualmente lo prevé la normatividad.

Estrategia:

Reconocimiento y protección adecuada de los Derechos Digitales y sus garantías, con la finalidad de garantizar la dignidad humana.

Líneas de acción:

- Promover y difundir en la ciudadanía incluyendo el ámbito escolar a partir de nivel básico, la existencia, objeto, alcance y límites del derecho de acceso a la información pública, de protección de datos personales y de los derechos digitales.

- Suscribir convenios de colaboración con la Secretaria de Educación Pública y las Secretarias de Educación de las Entidades Federativas para que en sus

programas y/o planes educativos se incluyan como temas de interés y relevancia los derechos ARCO y derechos digitales.

- Adoptar, aplicar y, de ser necesario, reformar leyes, reglamentos, políticas y medidas relativas a la protección en línea de los datos personales y la privacidad, a fin de prevenir, mitigar y remediar la recolección, retención, procesamiento, uso o la revelación arbitraria o ilícita de datos personales en internet.

- Establecer, implementar y hacer cumplir marcos legales integrales para proteger la privacidad y los datos personales de los ciudadanos, en observancia con las normas internacionales de derechos humanos.

Eje temático.

Consolidación del Convenio 108 Plus y el T-Mec

Justificación

La nueva versión del TLCAN ahora **T-MEC**, es resultado de la voluntad política, la visión y la flexibilidad que mostraron **México, Estados Unidos** y **Canadá** para lograr los balances necesarios y mantener el carácter trilateral del mismo.

La incorporación de México al Convenio 108 Plus (Convenio 108+) y la escasa eficiencia que han tenido los acuerdos internacionales entre EE.UU y la UE para la protección de datos personales, pueden tener efectos positivos para México ya que derivado del nuevo acuerdo comercial o tratado entre México, Estados Unidos y Canadá

(T-MEC) y la posición geográfica lo colocan como un país atractivo y competitivo para la inversión extrajera.

La Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, el Programa Nacional de Protección de Datos Personales y la adhesión de México al Convenio 108 en armonía con el Reglamento Europeo de Protección de Datos, la Ley Orgánica y Protección de Datos Personales y garantía de los derechos digitales y el Convenio 108 plus, facilitaría y garantizaría el **flujo seguro de datos personales** entre empresas ubicadas en la UE y México contribuyendo así considerablemente al desarrollo económico.

En el caso del comercio digital, el objetivo es establecer reglas horizontales que se apliquen al comercio realizado por medios electrónicos; para lo cual, las disposiciones pretenden cumplir tres objetivos principales: eliminar obstáculos injustificados al comercio realizado por medios electrónicos, otorgar certeza jurídica a los inversionistas y empresas y garantizar un entorno en línea seguro para los consumidores. En México se pretende fortalecer e impulsar el desarrollo del comercio digital mediante un esquema legal que fomente las operaciones electrónicas y, al mismo tiempo, brinde seguridad para los usuarios de los medios electrónicos y promover un entorno digital que favorezca operaciones por medios electrónicos seguros.

El **T-MEC** incluye disposiciones fundamentales para el desarrollo y funcionamiento del comercio digital, como lo es la **protección a los datos personales**, aranceles aduaneros, no discriminación de productos digitales, libre flujo de información, firmas electrónicas, ubicación no forzosa de servidores informáticos, entre otros; prevé esquemas legales y prácticas no discriminatorias para proteger la información personal

de los usuarios del comercio digital, a fin de generar confianza en la realización de las operaciones electrónicas; disposiciones para fortalecer la cooperación en temas relevantes como la ciberseguridad, a fin de identificar posibles amenazas en el entorno digital que afecten su sano desarrollo y, finalmente, facilitar el acceso y uso de los datos gubernamentales públicos, reconociendo su importancia para el desarrollo económico y social, para la competencia y la innovación.

Los beneficios para México consisten en fortalecer el desarrollo del comercio digital, impulsando la participación de las PyMEs mexicanas, establecer reglas que dan certeza jurídica al gobierno, al sector empresarial y a los consumidores, así como protección al uso de los datos personales, mantener un marco legal que rija las transacciones electrónicas y se identifican oportunidades de negocio en tecnologías de la información.

De igual manera, el objetivo de las **buenas prácticas regulatorias** es promover la transparencia y considerar los comentarios de los interesados y el público en general en todo el proceso regulatorio, requerir análisis fundamentados en evidencia y explicaciones de las nuevas regulaciones y alentar la cooperación regulatoria bilateral y trilateral.

Estrategia:

Fortalecer e impulsar el desarrollo del comercio digital mediante un esquema legal que fomente las operaciones electrónicas y, al mismo tiempo, brinde seguridad para los usuarios de los medios electrónicos.

Líneas de acción:

- Vigilar la protección de los datos personales que se generen en el flujo del

comercio digital, negocios e inversiones entre las empresas ubicadas en Estados Unidos, México y Canadá; para así dar seguridad a los productores, importadores e inversionistas sobre las medidas adoptadas para la protección de sus datos personales y su debida trasmisión.

- Implementar medidas y procedimientos para la protección de los datos personales de los productores, importadores e inversionistas, en el comercio digital, inversiones y negociaciones derivados del T-MEC; del sector de población de mayor vulnerabilidad o que han sido excluidos.

- Campañas de difusión, divulgación, capacitación o comunicación, a los entes que forman parte del sistema económico respecto de la materia de protección de datos personales y el intercambio efectivo y seguro de la información, que conllevan las prácticas comerciales en las que convergen productores, exportadores, importadores, inversionistas, entes como:

Eje temático.

El T-MEC y el Convenio 108 ante la caída de los Escudos de Privacidad, para hacer de México Puerto Seguro Sustituto del Flujo Transfronterizo de Datos Personales

Justificación

La Sentencia del Tribunal de Justicia (Gran sala), del 16 de julio del presente año, declara la invalidez de la Decisión de Ejecución (UE) 2016/1250 de la Comisión Europea de fecha 12 de julio de 2016, conforme con la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección proporcionada por el Escudo de Privacidad UE-EE. UU. Derivado de esta resolución, se detienen los flujos de información entre Estados Unidos y la Unión Europea, afectando a un sin número de empresas cuya información se almacenaba en servidores físicamente establecidos en territorio norteamericano. Esta resolución no solo afecta la relación de Estados Unidos y Europa, también puede afectar a empresas mexicanas que utilizan servidores norteamericanos, para el almacenamiento y tratamiento de sus bases de datos, por lo que el flujo transfronterizo podría requerirse que sea suspendido; afectando de manera significativa el Comercio Digital de México con Europa y con Estados Unidos.

Esta sentencia, tiene consecuencias importantes a nivel internacional ya que estas dos potencias económicas cuentan con la negociación de un Tratado de Libre Comercio (TLC) denominado Transatlantic Trade and Investment Partnership (TTIP) desde el año 2013. Este TLC entre la UE y EEUU se define en el siguiente contexto:

- Generaría en España hasta 143.000 puestos de trabajo.
- EEUU y la UE suman casi el 50% del PIB mundial y un mercado de más de 800 millones de consumidores.
- Entre EEUU y la UE podrían crearse 2 millones de empleos además de un aumento de los salarios globales de hasta un 0,5%.
- Más de 20 millones de compañías en la UE y 28 millones en EEUU son Pymes, lo que representa un 99% del total.
- El 80% del total de las ganancias potenciales del Tratado provienen de

la reducción de los costes impuestos en los reglamentos y de la liberalización del comercio de servicios y la contratación pública.

- Estados Unidos invierte en Europa tres veces más que en toda Asia, mientras que la UE lo hace en EE.UU. ocho veces más que en India y China juntas.

Instrumentos implementados para el Flujo Transfronterizo Comercio Europa – EEUU

Puerto Seguro

En el contexto sustantivo de la Economía Mundial del comercio entre la UE y EEUU, como se hizo referencia en el apartado previo, se buscó atender junto el Acuerdo Comercial del TTIP, la denominación de Puerto Seguro para garantizar la Protección de Datos en el Flujo Transfronterizo de la actividad comercial de la UE y EEUU. Distinguiendo a dicha denominación los siguientes aspectos.

- Con respecto a los principios de puerto seguro, cabe reseñar que constituyen un peculiar mecanismo, fruto de una prolongada negociación entre la Comisión y el Gobierno de EEUU, recogido en la Decisión de la Comisión 2000/520/CE de 26 de julio de 2000.
- Se trata de un instrumento singular que, tomando en consideración el contraste entre la autorregulación estadounidense y los estrictos criterios legales en materia de protección de datos de la UE, permite a las entidades de EEUU que lo deseen comprometerse a su cumplimiento, lo que tiene como consecuencia fundamental que respecto de las transferencias de datos personales dirigidas a esos concretos destinatarios se considera que EEUU es un país que proporciona protección adecuada

- Acreditar ante la AEPD que el destinatario se encuentra entre las entidades que se han adherido a los Principios; así como que se encuentra sometido a la jurisdicción de uno de los organismos públicos de EEUU que figuran en la mencionada Decisión 2000/520/CE.
- Entre las empresas adheridas al sistema de los principios de puerto seguro se incluyen los principales prestadores de servicios de redes sociales, motores de búsqueda y correo electrónico, respecto de los que resulta especialmente preocupante las revelaciones acerca de su eventual conexión con los programas de supervisión del Gobierno de EEUU.

La caída de la Denominación de Puerto Seguro

La declaración de invalidez de la Decisión 2000/520/CE de la Comisión relativa a los principios de Puerto Seguro (pieza fundamental del entramado que facilitaba las transferencias internacionales de datos desde la UE a EEUU), derivo sin duda de la demanda del Sr. Schrems que nunca dejo de pedir la declaración de invalidez de la Decisión 2000/520/CE de la Comisión relativa a los principios de puerto seguro.

Con respecto al funcionamiento de los artículos 25, 26 y concordantes de la Directiva, la principal aportación de la sentencia Schrems es que si bien cuando la Comisión ha adoptado una decisión que constata que un tercer país garantiza un nivel de protección adecuado –como sucede con la relativa al puerto seguro con respecto a EEUU- los Estados miembros y las autoridades nacionales de control no pueden adoptar medidas contrarias a la decisión, como establecer que el país en cuestión no garantiza un nivel de protección adecuado, sí cabe que la autoridad nacional de control conozca de reclamaciones relativas al tratamiento de datos transferidos con base en la decisión de la Comisión y que la validez de ésta sea revisada por el Tribunal de Justicia en el marco de una cuestión prejudicial planteada por un tribunal

nacional derivada de una de esas reclamaciones, como sucede con los tribunales irlandeses en el asunto Schrems

Invalidez de los principios de puerto seguro

El sistema de autocertificación instaurado carece de la necesaria fiabilidad, en la medida en que los principios de puerto seguro son aplicables únicamente a las entidades estadounidenses auto-certificadas, pero las autoridades de EEUU no quedan sometidas a esos principios, sin que la Decisión establezca cómo los EEUU a la luz de su legislación interna o sus compromisos internacionales garantizan esos principios.

En consecuencia, el Tribunal concluye que la Comisión no llevó a cabo una constatación debidamente motivada de que EEUU "garantiza efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de los derechos fundamentales sustancialmente equivalente al garantizado en el ordenamiento jurídico de la Unión". Además, destaca la sentencia que el artículo 3.1 de la Decisión priva a las autoridades nacionales de las facultades de control previstas en la Directiva, lo que determina que la Decisión 2000/520/CE vulnere las exigencias del artículo 25.6 de la Directiva y deba ser declarada inválida.

Tras la sentencia Schrems se abrió un incierto futuro, vinculado a las significativas diferencias entre los modelos de protección de datos prevalentes en EEUU y la UE, cuya coordinación se ve dificultada por las revelaciones relativas a las actividades de supervisión llevadas a cabo por las autoridades de EEUU. La inexistencia de un marco como el establecido en los principios de puerto seguro puede afectar de

manera significativa a la prestación de muchos servicios, que cada vez más se basan en la computación en nube.

Escudos de Privacidad

Ante la caída de la denominación de Puerto Seguro para el Flujo Transfronterizo de Datos, en 2016 se diseñó un nuevo mecanismo que permitirá continuar con este Flujo Comercial. Dichos Escudos de Privacidad, consagran los mismos principios de protección que el Acuerdo de Puerto Seguro; por lo que se sustentan en:

- Reglas más estrictas para transferir datos a terceros.
- Obligación de entregar a las autoridades copia de la política de privacidad empresarial, si aquéllas la requieren.
- Se refuerzan los mecanismos de solución de controversias (distintas fases; incluso se puede llegar al arbitraje).
- Cumplimiento de las reglas monitoreado por la FTC y las autoridades de PDP de los países europeos

Es importante mencionar que los Escudos de Privacidad, les permitieron a los países de Argentina y Uruguay poder firmar el Convenio 108 Plus; ya que estos se comprometieron a través de cláusulas tipo a la protección de los datos personales. Esto es un poco, como los esquemas creados para mantener las relaciones comerciales entre Estados Unidos y Europa, entendiendo la necesidad de principios de siglo; entendiendo que la naturaleza del país norteamericano no podría cambiar. En el caso de México desde el 2018, se adhirió al Convenio 108 y su protocolo adicional, además de cumplir con los términos y condiciones señalados por el Reglamento General Europeo; que trae como consecuencia que la materia de Protección de Datos Personales, se tome desde la perspectiva de un derecho

humanos y con ello, se incorpore al marco constitucional de los países; cumpliendo con las resoluciones Bruselas y Albania.

La Sentencia del Tribunal Europeo del 16 de julio del 2020

La Gran Sala Europea en su resolución ha establecido que no deberá permitirse, el uso de mecanismos para el flujo transfronterizo de datos con otros países, que no cumplan con los requerimientos para el debido tratamiento de los datos, establecidos por el Reglamento General Europeo de Protección de Datos. Por lo cual, Europa puede ampararse mediante el Convenio 108 y su protocolo adicional, ya que esta es la base esencial del Reglamento Europeo. Entonces bajo esta perspectiva, Europa tiene un tratado internacional, para el establecimiento de las directrices de la protección de los datos a través del flujo transfronterizo, con países fuera de la Unión Europea.

México, Puerto Seguro Sustituto para el Flujo Transfronterizo de la Unión Europa a México (Convenio 108 y su Protocolo Adicional) y México a Estados Unidos (T-MEC)

México, que por haberse adherido al Convenio 108 y su Protocolo Adicional (junio de 2018), tiene la categoría de ***Puerto Seguro (en la perspectiva que demanda la normativa del Reglamento General Europeo de Protección de Datos) y No de País Tercero***. Por lo tanto, es prioritario dar certeza y no permitir que se vulnere el comercio digital que se tiene por parte de empresas en México con empresas de la UE; ya el comercio digital representa el 0.5% del Producto Interno Bruto.

México es Puerto Seguro al contar con una legislación que reconoce a la protección de los datos personales como Derecho Fundamental; consecuencia de esto, todas

las instancias de gobierno están obligados a proteger este derecho; entre las que destacan el Órgano Garante Nacional (Inai) y los Órganos Garantes Estatales.

La protección de datos personales en el flujo transfronterizo, se da desde la Constitución Federal en los artículos: 1 (reconocimiento de Derechos Humanos), 6 (creación del Derecho a la Transparencia y Acceso a la Información, siendo una restricción para que por interés publico puedan ser vulnerados los datos personales; otorgando personalidad al Órgano Garante Nacional y Órganos Estatales), 16 segundo parrado (el reconocimiento del derecho a la protección de los datos personales). Bajo este contexto, la naturaleza del tratado internacional (Convenio 108 y protocolo adicional) firmado por México, obliga a que toda aquella información de carácter personal que provenga de la Europa, sea protegida bajo el esquema de un derecho humano.

Una vez, que la información llega a México consolidándose la actividad social o económica en este vértice; se inicia con una perspectiva de la protección del dato personal como esquema económico. Esto se da en virtud de que nuestro país, tiene una relación económica con los países de Estados Unidos y Canadá (T-MEC), lo que tiene como resultado que el tratamiento de los datos no se vea como un derecho humano; sino bajo una perspectiva de reglas de origen que se da entre los países miembros.

Por ello, al referirse a la materia de Protección de Datos Personales en el T-MEC, no se debe interpretar de carácter limitativo en su capítulo 32 de excepciones y disposiciones generales, en su artículo 32.8 referente a la protección de información personal; debido a la existencia de diversas disposiciones en la materia en los capítulos 17, 18, 19 y 20 en este documento:

El T-MEC, lleva a cabo un blindaje a través de los cinco Capítulos (capítulo 17 de los Servicios Financieros, capítulo 18 de las Telecomunicaciones; capitulo 19 Comercio Digital; capítulo 20 de los Derechos de Propiedad Intelectual y capitulo 32 de las Excepciones y Disposiciones Generales, en materia de la Privacidad u Protección de los Datos Personales), que conforman el marco regulatorio sobre el tratamiento de los datos personales, en las relaciones entre estos tres países; que puede ser utilizado como mecanismo de flujo transfronterizo de información.

Este esquema del T-MEC, permite visualizar a México como un país receptor, cuyo objetivo será que las operaciones de tratamiento de datos de las empresas trasnacionales, no sigan su flujo a Estados Unidos sino estas, pueda llevarse a cabo en nuestro territorio. Ahora bien, este esquema con el uso de reglas de origen (establecer de donde es el producto), haciendo que las empresas trasnacionales de Estados Unidos y Canadá, tengan seguridad de las operaciones que se llevan a cabo (tratamiento de datos personales); sin generar con ello, la vigilancia por parte de las Agencias de Seguridad.

En este contexto, se determina que la protección de los datos personales a la luz del T-MEC, se encuentra bajo la visión de la seguridad de la información; por ello, se da esta protección en los sistemas financieros, telecomunicaciones, comercio digital y propiedad intelectual. Por ello, que este cuidado de la información, se da mediante capas de protección que permiten llevar a cabo el flujo transfronterizo de los datos, sin ser vulnerada la información.

Ahora bien, si se realizara **un análisis de las cláusulas de la figura de Escudos de Privacidad celebradas entre Europa y Estados Unidos, no podríamos encontrar los esquemas de seguridad que ofrece México en sus dos vertientes**

ante el flujo de información (como derecho fundamental y como relación económica), que resultan difícil de evadir o vulnerar. Por ello, las cláusulas de los escudos de privacidad presentaban diversos tipos de vulneraciones, al enfrentarse cuestiones como: seguridad nacional, lagunas de interpretación, atribuciones de agencias.

Por esta razón, el propio acuerdo comercial del T-MEC da la certeza a sus estados miembros que, en el momento de existir una violación, vulneración o incidente, en la seguridad del flujo transfronterizo de datos; estos, podrán acudir a instancia o tribunales internacionales, para dirimir controversia al respecto.

Estrategia

Hacer de México un Puerto Seguro para el Flujo Transfronterizo de la Unión Europa a México

Líneas de acción:

- Proteger a las empresas amenazadas por la Sentencia del 16 de julio del presente año, por la Gran Sala del Tribunal Superior Europeo, al dejar inválidos a los escudos de seguridad. Estableciendo que México, es un puerto seguro por las condiciones de armonización que tiene con el Convenio 108 y su Protocolo Adicional. Aquellas empresas que representan ese cinco por ciento del comercio digital, que se encuentran sosteniendo la economía de este país,

- Determinar de manera precisa que México, cuenta con el tratado de México, Estados Unidos y Canadá (T-MEC), que le otorga los niveles de seguridad adecuados para las relaciones comerciales entre los países miembros. Dando protección en los sistemas financieros, telecomunicaciones, comercio digital y propiedad intelectual; además de encontrarse con la aprobación de los poderes Ejecutivo y Legislativo.

- Incentivar, a empresas mexicanas a constituirse de manera legal y convertirse en parte de la cadena productiva en el Comercio Digital, con acciones para que incorporen su actividad al trabajo con tecnologías de la información; Pudiendo tener la intervención del Gobierno o en su caso, inversión de la iniciativa privada. Reactivando a las empresas con la cadena productiva de Estados Unidos y Europa. En este sentido, lograr que las empresas mexicanas, tengan la facultad de recibir el flujo transfronterizo de datos de Europa a México amparado por el convenio 108 y su protocolo adicional en su modalidad de puerto seguro. Al consolidarse en la actividad comercial de los datos en México, estar en posibilidades de establecer flujo transfronterizo de datos con las empresas de Estados Unidos bajo el amparo del T-MEC.

- Establecer de manera real el derecho a las tecnologías de la información e internet, contemplado en el Plan Nacional de Desarrollo, con el objetivo de contar con infraestructura a nivel Federal, Estatal y Municipal, como inversión masiva. Para que las Unidades Económicas tengan lo propio, en el contexto de infraestructura y competencias, para convertirse en receptoras de los flujos transfronterizos de datos. Así mismo, estas unidades económicas, pueden prestar servicios a aquellas empresas que cuenten con centros de datos en todo el país, para que al amparo del Capítulo de Reglas de Origen del T-MEC,

las fases de tratamiento de bases de datos de empresas de EEUU, traigan sus etapas de producción en alguna de las entidades federativas de México, al igual que en 1994 se dio el desarrollo de la Industria Maquiladora de Exportación que aprovecho la mano de obra calificada más barata que se tenía en México. Lo cual representan para México Inversión Extranjera Directa, generación de empleo y cumplir con la Cortinas de Desarrollo Regional que ha priorizado el Gobierno Federal en el Plan de Nacional de Desarrollo 2019-2024, y que sin duda lograría una efectiva reactivación de la economía en México.

- Certificar especialistas en Protección de Datos Personales, para ello se deberán implementar programas académicos, programas de capacitación, programas de interiorización a las empresas, con perspectiva de derecho humano y con perspectiva de protección en materia de comercio digital. Como resultado de estos programas certificar a los Oficiales de Protección de Datos Personales.

Eje temático.

Portabilidad de datos personales.

Justificación.

El embate tecnológico, que actualmente acontece en México, vislumbra un crecimiento de manera exponencial en comparación con años anteriores, esto derivado de que por la crisis de salud pública actual, por la emergencia de sanitaria covid_19, la gran

mayoría de nuestra vida social, educativa, laboral y económica se ha desarrollado a través de estas plataformas .Según cifras del INEGI, con datos del año 2019, publicados en febrero de 2020, señala que en México somos 80.6 millones de usuarios de Internet, que representan el 70.1% de la población de seis años o más. El empleo y uso de internet y plataformas digitales además de generar oportunidades de crecimiento entre los usuarios trae consigo ciertos riesgos.

Esta explosiva expansión del uso de internet ha traído consigo también una serie de retos y desafíos en el reconocimiento y protección de derechos, el vínculo entre derechos fundamentales y las tecnologías requiere de normatividad y políticas públicas encaminadas a castigar o penalizar cualquier tipo de vulneración de estos derechos.

Ante el fenómeno que se vive, la Comisión IDH publicó la resolución 1/2020 titulada Pandemia y derechos humanos en las Américas, en dicha resolución se hace un llamado a las autoridades Para enfrentar a la pandemia del COVID 19, como asunto público, exige que la gente esté informada y el derecho a la información está ahí. En la misma determinación, hace un llamado a los órganos que garantizan estos derechos, pues se debe otorgar prioridad a las solicitudes de acceso a la información relacionadas con la emergencia de salud pública, y se debe priorizar la protección a la vida privada de las personas en este contexto de emergencia.

Proteger el derecho a la privacidad y los datos personales de la población, especialmente de la información personal sensible de los pacientes y personas sometidas a exámenes durante la pandemia. Los Estados, prestadores de salud, empresas y otros actores económicos involucrados en los esfuerzos de contención y tratamiento de la pandemia, deberán garantizar los derechos de Acceso, rectificación, cancelación, oposición y portabilidad de datos personales, es a esta última a la que me quiero referir.

Portabilidad

El concepto de portabilidad atiende a diversas connotaciones, en principio este término fue acuñado en (2006) por la universidad de Sevilla, definiéndola como la "capacidad que deben tener las aplicaciones para ser ejecutadas en distintos sistemas informáticos es decir que debe existir *interoperabilidad*,(característica propia de los sistemas o componentes para intercambiar información entre sí)[6] es de esta manera que nace el significado de portabilidad, en un primer momento como un término netamente informático pero que más tarde se traslada al mundo empresarial obedeciendo al contexto de la competencia económica.

En esta misma línea, el concepto de portabilidad nos remite a una segunda vertiente la de *portabilidad referida* también conocida como *portabilidad numérica* misma que es impulsada por las autoridades en materia de telecomunicaciones con la finalidad de promover mayor competencia y bienestar para los consumidores, éste tipo de portabilidad permite a los usuarios de telefonía móvil cambiar de proveedor de servicio sin perder su número telefónico y así reducir los llamados *switching costs* o gastos que representa el tener que cambiar de proveedor, producto o servicio. (Aguilar, 2012)

Ahora bien, dentro del concepto portabilidad numérica podemos encontrar algunas variantes entre las cuales se pueden destacar las siguientes:

Portabilidad numérica frente a proveedor del servicio: Suscriptores pueden cambiar el proveedor del servicio reteniendo el mismo número telefónico.

Portabilidad numérica frente a ubicación geográfica: Suscriptores pueden cambiar su ubicación geográfica mientras mantienen el mismo número de teléfono.

---

[6] Guía de implementación de la facilitación del comercio. Comisión Económica de las Naciones Unidas para Europa. CEPE/ONU.

Portabilidad del servicio: Suscriptores pueden cambiar los servicios contratados con el operador mientras mantienen el mismo número telefónico. (Yi-Bing Lin, 1999 citado en Vásquez, 2010).

Así mismo, con la implementación de la portabilidad referida en el ámbito empresarial el beneficio que tiene en los consumidores es incosteable ya que dejan de pagar los gastos que trae consigo el cambio de compañía que le brinda el servicio y pueden trasladar todos sus datos relativos al número telefónico que le fue asignado a otra empresa que se hará responsable de proporcionar la misma prestación y sin que el usuario tenga que pagar algo por el traslado de su información.

Portabilidad en la Unión Europea

Sin duda alguna, hablar de portabilidad en el ámbito del derecho necesariamente nos remite a hablar del derecho a la protección de los datos personales[7] junto con sus distintas modalidades como lo son el acceso, rectificación, cancelación y oposición al tratamiento de datos personales, mejor conocidos como derechos ARCO, conceptos íntimamente ligados que tienen como finalidad en todo momento el garantizar a usuarios de las tecnologías la más amplia protección de sus datos personales en el mundo digital.

Es así, bajo este contexto de la protección de datos personales que en la matriz del Parlamento Europeo, durante el año 2012, surge la idea de realizar la portabilidad de los datos personales y reglamentarla en el artículo 18 de la primera propuesta del Reglamento General de Protección de Datos UE, que más tarde fue modificado y aprobado en 2016 quedando como *"Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre*

[7] Se considera como Dato Personal a la información concerniente a una persona física o jurídica colectiva identificada o identificable, establecida en cualquier formato o modalidad, y que esté almacenada en los sistemas y bases de datos.

circulación de estos datos y por el que se deroga la Directiva 95/46/CE, es en este nuevo documento que se describe mejor el formato en el que se realiza el tratamiento de los datos personales para realizar la portabilidad.

Dentro de lo establecido en el artículo 20 primer apartado del reglamento referente al derecho de portabilidad señala que:

"El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento[8], en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado. (RGPD UE 2016/679: 2016)

Así mismo, en las directrices del reglamento se expresa que el derecho a la portabilidad surge como una herramienta que respalda la libre circulación de los datos personales ya que promueve la competencia entre los responsables del tratamiento, además de facilitar el cambio entre distintos proveedores de servicio promoviendo así el desarrollo .de nuevos servicios en el mercado digital.

Resulta importante señalar que el modelo europeo de portabilidad de datos personales únicamente se establece para el sector privado ya que su objetivo (como en la portabilidad numérica) es fomentar la igualdad de condiciones en la competencia económica, por ende las personas pertenecientes a la Unión Europea únicamente pueden solicitar la copia de sus datos o la transmisión de los mismos a empresas del ámbito privado.

Portabilidad en México

Como hemos visto en líneas anteriores, la inclusión de la portabilidad en los sistemas jurídicos actuales obedece a transformaciones sociales culturales y tecnológicas, que

[8] Debe entenderse por Responsable de Tratamiento: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento de los datos personales.

nacen en el seno de postulados internacionales basados en políticas de libertad, respeto, promoción y protección a los derechos humanos.

De este modo en México durante el año 2009 se plasmó en la Constitución Política de los Estados Unidos Mexicanos el derecho la protección de datos personales, posteriormente, en 2015 se reforman las leyes en materia de transparencia y es hasta 2017 que se emite la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en donde se redefinió lo planteado por la Unión Europea en cuanto a la regulación de la portabilidad de los datos personales pero en este caso se aplicó al sector público estableciendo que los sujetos obligados de la administración pública federal, estatal o municipal fueran los responsables en el ejercicio de la portabilidad, en este marco el artículo 57 fracción I y II, menciona de manera expresa que :

“Cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos.”

Así mismo manifiesta que cuando el titular haya facilitado los datos personales y el tratamiento se base en el consentimiento o en un contrato, tendrá derecho a transmitir dichos datos personales a otro sistema, sin impedimento por parte del responsable. (LGPDPPSO: 2017)

Por lo tanto, puede decirse simplificadamente que la introducción de la portabilidad a la ley general en materia de protección de datos personales implica que todas las instituciones, organismos auxiliares, organismos autónomos, partidos políticos, ayuntamientos, fideicomisos públicos en el ámbito de su competencia que posean cualquier información concerniente a una persona física que la haga identificada o

identificable[9], es decir que tengan sus datos personales, como pueden ser el nombre, la fotografía, domicilio, datos biométricos[10], RFC, CURP, entre otros a través de los cuales una persona pueda ser reconocida, deberán garantizar a los titulares de esos datos la portabilidad de los mismos a través de un formato que sea interoperable o compatible con diferentes sistemas, para que el titular pueda tener una copia y pueda seguir utilizándolos o transmitirlos a otro responsable.

Ahora bien garantizar la portabilidad en el sector público parece poco tangible, ya que en ningún otro país ha sido impulsada, sin embargo el concepto de interoperabilidad que se liga estrechamente a la portabilidad, ya se ha venido trabajando desde el año 2011, a través del llamado Gobierno Digital[11], en donde se establecieron esquemas de interoperabilidad y datos abiertos en la administración pública para incrementar la eficiencia operativa de la misma, por lo que implementarla en el sector gubernamental dejaría grandes ventajas en todos los niveles.

Beneficios y ventajas de la portabilidad en México

Es indiscutible que el uso adecuado y la buena conducción de la portabilidad de los datos personales traería consigo dos ventajas importantes a saber: la primera, disminuir los costos (tiempo y dinero) en los trámites de carácter personal que realicen los titulares de los datos en cualquier instancia del sector público, dado que para realizar cualquier trámite lo primero que se tiene que hacer es acreditar la personalidad por medio de documentos que la misma administración pública emite, por lo que al ejercer

---

[9] Se estima que una que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

[10] Deberá entenderse por datos biométricos aquellos rasgos físicos, biológicos o de comportamiento de un individuo que lo identifican como único del resto de la población.

[11] Se concibe como Gobierno digital: a las políticas, acciones y criterios para el uso y aprovechamiento de las tecnologías de la información y comunicaciones, con la finalidad de mejorar la entrega de servicios al ciudadano; la interacción del gobierno con la industria; facilitar el acceso del ciudadano a la información de éste, así como hacer más eficiente la gestión gubernamental para un mejor gobierno y facilitar la interoperabilidad entre las dependencias y entidades;". Fracción XVI del artículo segundo del Acuerdo por el que se establece el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal.

el derecho de portabilidad el titular podría llevar a la dependencia o solicitar el traslado de la información de una institución a otra. Por todo ello, es sumamente importante contemplar la necesidad de hacer efectivo este derecho, ya que, el contexto de la pandemia nos obliga a implementar todos los mecanismos necesarios para enfrentar la crisis de salud que vivimos.

La segunda ventaja implica la disminución de la burocracia y la corrupción que genera el realizar los trámites administrativos u obtener una copia de los documentos personales de los titulares, ya que como lo demuestran estudios estadísticos la corrupción permea el ámbito burocrático ejemplo de ello es el Índice de Percepción de la Corrupción 2017 en el cual México ocupo el lugar 135 de 180 del ranking[12], del mismo modo en la Encuesta Nacional de Calidad e Impacto Gubernamental (ENCIG) 2017 donde se reveló que a nivel nacional el 91.1% de las personas encuestadas refirió que los actos de corrupción en la realización de trámites son muy frecuentes y la tasa estimada de víctimas de la corrupción en las gestiones fue de 14,635 por cada 100 mil habitantes; en consecuencia la corrupción es un problema que se podría combatir al garantizar la portabilidad de los datos personales la tarea de hoy en día es que la ciudadanía esté informada para exigir el ejercicio de esta nueva modalidad del derecho, pues el costo de la corrupción asciende a los siete mil doscientos dieciocho millones de pesos, equivalente a dos mil dos cientos setenta y tres pesos por cada víctima, de acuerdo con la ENCIG 2017.

A partir de la emisión de la Ley General y la Ley Federal, se ha buscado implementar la manera más eficiente de implementar e instrumentar a través de la Plataforma Nacional de Transparencia la portabilidad de los datos personales, por lo que ha emitido los respectivos lineamientos para la tramitación de solicitudes y medios de impugnación que atiendan a dicho derecho, aunado al hecho de que sin duda alguna se ha requerido

[12]Datos recogidos por Transparency International the global coalition against corruption en 2017

de un gran trabajo interdisciplinario que congregó a los expertos en distintas materias como lo son la informática, ingeniería en desarrollo de sistemas, jurídicos, etc.; para lograr que dicha plataforma sea interoperable y abastezca a todo el país así como a sus sujetos obligados.

Sin embargo, la Plataforma Nacional no ha conseguido poner en marcha todas las medidas de seguridad necesarias para dar vida al ejercicio del derecho a la portabilidad de los datos personales, ya que se trata de la posibilidad de brindar a los particulares toda la información respecto de su persona que se encuentre en posesión de los sujetos obligados, por lo que requiere de la mayor protección en contra de las amenazas cibernéticas que pudieran vulnerar a la plataforma.

Por lo cual, de un análisis general entre los 32 Órganos Garantes, se advierte que el Estado de México ha invertido en una plataforma electrónica capaz de garantizar todas las medidas de seguridad que la Ley Genera, Ley Local y Lineamientos han determinado para la portabilidad, convirtiéndose en el modelo a seguir para la implementación de los demás sistemas. El Sistema de Acceso, Rectificación, Cancelación y Oposición de Datos Personales del Estado de México (SARCOEM) facilita la recepción, trámite y seguimiento de los llamados derechos ARCO y la portabilidad, ya que como se ha mencionado cuenta con los mayores niveles de seguridad pues los archivos que se suben a esta plataforma y se envían se encriptan automáticamente y cuenta con el protocolo seguro de su “https”, por lo que no cuenta únicamente con estándares de carácter nacional sino de orden internacional para el manejo de datos personales.

El SARCOEM, se ha presentado como un sistema que cumple con tres niveles de seguridad para mitigar los posibles riesgos de una amenaza, los cuales para poder vulnerar y/o violentarlos es necesario que el atacante cuente con distintos factores como grandes recursos económicos, tiempo, conocimientos técnicos especializados e

infraestructura tecnológica costosa, debido a que los niveles de seguridad son: 1º se conforma por dos hardware, el primero es el Fortywall encargado de detectar ataques, el segundo es el Firewall el cual bloquea los ataques externos, 2º la utilización del certificado HTTPS, en donde la información que se envía a través de este dominio viaja encriptada y 3º los archivos que se envían están cifrados por el sistema desarrolla en el propio INFOEM, dicho cifrado consta de 512 caracteres. (4000 bits); razones por las cuales se considera un modelo a seguir para la implementación de dicho derecho.

En tiempos como los de ahora, en donde los gobiernos optan por la vigilancia der sus gobernados, garantizar la portabilidad significaría para las personas regresarles el poder de conocer y decidir sobre los datos que las instituciones públicas recolectan de su persona, sin dejarlos en un estado de vulnerabilidad.

Estrategia:

Delimitar sus alcances y objetivos, así como la implementación de procesos tecnológicos y normativos que otorguen certeza a los ciudadanos y al mismo tiempo homologue las actuaciones de los organismos garantes en el ejercicio de esta prerrogativa.

Líneas de acción:

- Difundir al pueblo Mexicano a través de los diversos medios de comunicación y difusión, la portabilidad de datos personales como una opción más que se encuentran dentro de sus derechos.

- Es importante que los sujetos obligados adopten herramientas, aplicaciones o servicios tecnológicos que permitan una eficiente comunicación de los datos personales, es decir, tender hacia el uso de formatos estructurados y

comúnmente utilizados.

- Adopción de protocolos de seguridad estrictos por parte de los organismos garantes, esto con la finalidad de evitar la difusión de datos personales de manera irresponsable, tanto por medios de comunicación, sectores gubernamentales o de carácter privado.

- Establecer mecanismos de seguimiento que faciliten al responsable del tratamiento verificar que el envío, la recepción e incluso, la integridad de los datos personales objeto de dicha modalidad fueron adecuados y oportunos.

- Conocer que datos se encuentran en posesión de un tercero, al igual que su estado, corregirlos si son inexactos o desactualizarlos, pedir su suspensión o eliminación cundo su uso no corresponda a lo estipulados y negarse al tratamiento, o exigir su cese.

- Realizar capacitaciones constantes a los sujetos obligados para que exista una plena interoperabilidad de sistemas para garantizar el derecho de la portabilidad de datos personales.