Senado de la República, D.F. 28 de abril de 2016

SENADOR ROBERTO GIL ZUARTH
PRESIDENTE DE LA MESA DIRECTIVA
DEL SENADO DE LA REPÚBLICA
PRESENTE.

Quien suscribe, Senadora Dolores Padierna Luna, integrante del Grupo Parlamentario del Partido de la Revolución Democrática, a la LXIII Legislatura del Congreso de la Unión, con fundamento en lo dispuesto por los artículos 200, numeral 1, y 201 del Reglamento del Senado de la República y con referencia al **Dictamen de las comisiones unidas de Gobernación y de Estudios Legislativos Primera, con proyecto de decreto por el que se expide la Ley General de Protección de Datos Personales en posesión de sujetos obligados** someto a la consideración de esta soberanía las siguientes propuestas de adiciones y modificaciones para quedar como siguen:

Consideraciones

1. Se propone la inclusión del término de "Portabilidad de datos" en el artículo 3.

Cabe señalar que de la lectura del artículo 57 se desprende que esa transferencia de datos se podrá realizar siempre y cuando se tenga el mismo formato electrónico. De ahí, la importancia de definir claramente que se debe entender por portabilidad de datos.

Si bien el artículo 57 utiliza los términos "formato estructurado y comúnmente utilizado"; lo cierto es que los datos se dividen en dos tipos: (i) los estructurados y (ii) los no estructurados. Cuando se habla de datos estructurados se hace referencia a las bases de datos (sistematización de información personal); mientras que cuando se habla de datos no estructurados se refiere a archivos planos (comúnmente conocidos como objetos en diversos formatos tales como: .PDF; .DOC. XML; entre otros). Por esa razón consideramos que es necesario que la Ley General cuente con una definición clara sobre la portabilidad de los datos (el formato o tipo usado para la transferencia de datos).

DICE	DEBE DECIR
Artículo 3. Para los efectos de la presente Ley se entenderá por: **I. Áreas:** Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento, y ser	... ...

responsables o encargadas de los datos personales; **II. Aviso de privacidad:** Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos; **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; **IV. Bloqueo:** La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda; **V. Comité de Transparencia:** Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública; **VI. Cómputo en la nube:** Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente; **VII. Consejo Nacional:** Consejo Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales a que se refiere el artículo 32 de la Ley General de Transparencia y Acceso a la Información Pública; **VIII. Consentimiento:** Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos. **IX. Datos personales:** Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información; **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;	
XI. Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales;	...
XII. Días: Días hábiles;	...
XIII. Disociación: El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo;	...
XIV. Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee;	...
XV. Encargado: La persona física o **jurídica, pública o privada, ajena a la organización del responsable,** que sola o conjuntamente con otras trate datos personales **a nombre y** por cuenta del responsable;	...
XVI. Evaluación de impacto en la protección de datos personales: Documento mediante el cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable;	...
XVII. Fuentes de acceso público: Aquellas bases de datos, sistemas o archivos que por disposición de ley puedan ser consultadas públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso, el pago de una contraprestación, tarifa o contribución. No se considerará fuente de acceso público cuando la información contenida en la misma sea obtenida	...

o tenga una procedencia ilícita, conforme a las disposiciones establecidas por la presente Ley y demás normativa aplicable; **XVIII. Instituto:** Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales; el cual es el organismo garante de la Federación en materia de protección de datos personales en posesión de los sujetos obligados.	...
	XIX. Portabilidad de los datos: soluciones tecnológicas que permiten con mayor facilidad transferir todos sus datos personales desde un proveedor o plataforma tecnológica a otro garantizando la disponibilidad de los datos personales y la continuidad del servicio nacional o internacional;
XIX. Medidas compensatorias: Mecanismos alternos para dar a conocer a los titulares el aviso de privacidad, a través de su difusión por medios masivos de comunicación u otros de amplio alcance; **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 mas 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	(se recorre la numeración)

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; **XXIV. Organismos garantes:** Aquellos con autonomía constitucional especializados en materia de acceso a la información y protección de datos personales en términos de los artículos 6o., 116, fracción VIII y 122, apartado C, BASE PRIMERA, fracción V, inciso ñ) de la Constitución Política de los Estados Unidos Mexicanos; **XXV. Plataforma Nacional:** La Plataforma Nacional de Transparencia a que hace referencia el artículo 49 de la Ley General de Transparencia y Acceso a la Información Pública; **XXVI. Programa Nacional de Protección de Datos Personales:** Programa Nacional de Protección de Datos Personales; **XXVII. Remisión:** Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano; **XXVIII. Responsable:** Los sujetos obligados a que se refiere el artículo 1 de la presente Ley que deciden sobre el tratamiento de datos personales; **XXIX. Sistema Nacional:** El Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales; **XXX. Supresión:** La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas	

por el responsable; **XXXI. Titular:** La persona física a quien corresponden los datos personales; **XXXII. Transferencia:** Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado; **XXXIII. Tratamiento:** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, y **XXXIV. Unidad de Transparencia:** Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública;	

2. Con el fin de lograr una mayor claridad, en los alcances de los principios contemplados en el Artículo 16 de la Ley, se propone dar una definición de cada uno de estos; se ha decidido su inclusión, ya que en la praxis, en el proceso de implementación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y de la Ley de Protección de Datos Personales para el Distrito Federal, al no definirse los sujetos obligados tuvieron complicaciones para determinar con claridad la forma de implementarlos.

Un ejemplo de lo anterior, sería la imperiosa necesidad en la que se vio el Instituto de Acceso a la Información y Protección de Datos Personales de la Ciudad de México (INFODF), que a meses de haber sido publicada en la Gaceta Oficial la Ley de Protección de Datos Personales para el Distrito Federal, ante las peticiones que se recibieron de los entes obligados sobre la necesidad de determinar los alcances de los principios ahí contemplados, por lo que emitió los Lineamiento para la Protección de Datos Personales en el Distrito Federal.

Bajo esa tónica se propone, que la redacción del artículo 16 de la Ley, sea la siguiente:

DICE	DEBE DECIR
Artículo 16. El responsable deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamientos	**Artículo 16. El responsable y en su caso el encargado del tratamiento deberán observar los siguientes principios:**

de los datos personales.	**Principio de proporcionalidad, en virtud del cual los datos de carácter personal sólo se podrán recolectar y someter a tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y los propósitos o finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.** **Principio de calidad de los datos, en virtud del cual los datos personales deberán ser exactos, completos y actuales, en relación con el propósito para el cual serán utilizados.** **Principio de especificación del propósito o finalidad, en virtud del cual el propósito de la recolección de datos personales se deberá especificar, en los casos en que se requiera el consentimiento, a más tardar en el momento en que ésta se produce, y en cada momento en que se realiza un cambio de propósito.** **Principio de limitación de uso, en virtud del cual el tratamiento de los datos personales se verá limitado al cumplimiento de los propósitos de su recolección, y no se deberán tratar tales datos, excepto si se tiene el consentimiento del titular o lo dispone la normatividad en la materia.** **Principio de seguridad de los datos, en virtud del cual los responsables del tratamiento de datos personales emplearán las medidas técnicas y organizativas adecuadas a los riesgos que presenta el tratamiento, tales como pérdida, o acceso, destrucción, uso, modificación o divulgación de los mismos, cuando estas acciones no hayan sido autorizadas.** **Principio de acceso y oposición, en virtud del cual el titular o interesado tienen el derecho a obtener información de todos los datos relativos a su persona que consten en un registro o base de datos, y a oponerse a su tratamiento cuando no haya justificación legal para él.** **Principio de transparencia, en virtud del cual debe informarse al titular de los datos personales, acerca del objetivo del tratamiento y la identidad del responsable del registro o base de datos.** **Principio de acceso a información, en virtud del cual el titular tiene derecho a que se le**

	comunique en cada recolección de datos personales, de manera expresa, precisa, clara, inequívoca y gratuita, la información que los responsables del registro o base de datos deben suministrarle en conformidad a la normatividad en la materia.

3. Considerando que muchos de los sistemas de datos personales que se encuentran en poder de los sujetos obligados pueden ser adquiridos de manera fraudulenta por terceros y que el propio sujeto obligado, en múltiples trámites desconoce la buena fe del peticionante, es que se propone, en el **Artículo 23**, la adición del **principio de buena fe** y la posibilidad de que el responsable o encargado puedan ser relevados del deber de secreto, que se encuentra hermanado con el principio de confidencialidad por una orden judicial.

Un ejemplo de lo anterior sería cuando un Ministerio Público, para determinar una determinada conducta tipificada en el Código Penal del Estado, solicita al Juez que requiera al ente obligado que bajo su control se encuentra el sistema de videovigilancia de la zona.

Siguiendo la lógica planteada por la Ley, toda información relacionada con una persona física identificada o identificable debe ser guardada bajo confidencialidad, en tal sentido, la o las imágenes captadas por un sistema de videovigilancia se consideran datos personales, los cuales no pueden ser revelados a terceros; sin embargo, en este caso con la existencia de la orden judicial, el ente obligado que cuenta con la información podrá revelarla sin incurrir en las responsabilidades contempladas en la Ley, por el principio de buena fe.

DICE	DEBE DECIR
Artículo 23... Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por el titular y hasta que éste no manifieste y acredite lo contrario. Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos. ...	**Artículo 23...** Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por el titular y hasta que éste no manifieste y acredite lo contrario. **Lo anterior bajo el principio de buena fe.** Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos. ...

4. Tomando como referencia la reciente filtración del **padrón electoral,** es que se propone que las brechas de seguridad, a las que se refiere el **artículo 40**, no se circunscriban exclusivamente a los derechos patrimoniales o morales, sino que también a los datos sensibles.
   - En materia electoral, se propone que se incluya la obligación de las autoridades electorales de informar las brechas de seguridad que afecten al padrón electoral.
   - De igual manera en materia de educación cuando se vea afectado el Registro Nacional de Profesiones.

Lo anterior en virtud de que en la historia reciente de nuestro país, denota que estos dos últimos registros nacionales son los más afectados por vulneraciones a sus niveles de seguridad; afectando a miles de mexicanos.

Es conocido por todos y se ha documentado por la prensa escrita, que por lo menos en la Ciudad de México, existen diversas zonas en las que se pueden comprar: el padrón electoral, el de licencias, el de profesiones, e incluso se puede mandar a fabricar títulos profesionales apócrifos o comprar una identidad; así mismo, la semana pasada el Instituto Nacional Electoral tuvo una brecha de seguridad, que liberó todo el padrón electoral y alguna otra información que se encuentra adminiculada a está y se publicó en AMAZON. Aunque el portal en cuestión baje, suprima, cancele o elimine ese listado miles de mexicanos han sido afectados.
Sin embargo, más allá de la nota periodística y reportajes televisivos los miles de afectados, por esas brechas de seguridad que ponen en peligro nuestra seguridad, no hemos sido informados; esto en virtud de que actualmente **no es una obligación de esos entes de informar tal situación.**

En el caso, de que se dejaré la redacción tal como se encuentra en el dictamen, en la que se impone el deber de informar en caso de que los datos personales involucrados en la brecha de seguridad sean de tipo patrimonial o moral, la sociedad mexicana no podrá tomar las medidas de seguridad adecuadas, cuando sus datos de tipo electorales –que incluyen los identificativos- o de tipo académicos se vean afectados.

DICE	DEBE DECIR
Artículo 40. El responsable deberá informar sin dilación alguna al titular, y según corresponda, al Instituto y a los organismos garantes de las entidades federativas, las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales, en cuanto se confirme que ocurrió la vulneración y que el responsable haya empezado a tomar las acciones	Artículo 40. El responsable deberá informar al titular, al Instituto y los organismos garantes, según corresponda, las vulneraciones que afecten **datos sensibles y** de forma significativa sus derechos patrimoniales o morales, en cuanto confirme que ocurrió la vulneración y haya tomado las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la

encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos	afectación, y sin dilación alguna, a fin de que los titulares afectados puedan tomar las medidas correspondientes. **Así mismo, los responsables en materia electoral, deberán informar al titular, al Instituto y los organismos garantes, según corresponda, las vulneraciones que afecten los datos personales que obren en el padrón electoral o en el de militantes, esto en los términos fijados en el párrafo anterior.** **En el caso de Secretaría de Educación Pública, deberá informar al titular y al Instituto, las vulneraciones que afecten los datos personales que obren en el Registro Nacional de Profesiones.**

5. Dentro de los requisitos para presentar una solicitud ARCO **(artículo 49)**, se señala que estas pueden ser presentados por un representante, sin embargo, no se dice cómo será esa representación. Por lo que se propone la inclusión de que ese acto sea por medio de carta poder, firmada ante dos testigos o poder expedido por fedatario público, a fin de que el o los titulares de datos personales que no puedan o no sea su deseo, presentar directamente la solicitud ARCO, o en su caso recoger la respuesta recaída, sepan cuáles son los mecanismos que se debe emplear para su representación.

Por ejemplo, en la Ley de Protección de Datos Personales para el Distrito Federal, esta ambigüedad también se encuentra presente. Esta ambigüedad ha sido utilizada por algunos sujetos obligados, requiriendo que los documentos que acrediten la representación sean por medio de instrumento notarial, nulificando la posibilidad de gran parte del sector poblacional la obtención de esa información, u obligándolos a trasladarse hasta la oficina correspondiente.

DICE	DEBE DECIR
Artículo 49. Para el ejercicio de los derechos ARCO será necesario acreditar la identidad del titular, y en su caso, la identidad y personalidad con la que actúe el representante.	Artículo 49. Para el ejercicio de los derechos ARCO será necesario acreditar la identidad del titular, y en su caso, la identidad **y** personalidad con la que actúe el representante, **lo cual, podrá realizarse por medio de carta poder firmada ante dos testigos, o poder expedido por fedatario público.**

6. A raíz de los avances tecnológicos surge el tema del derecho al olvido (Cancelación y Oposición) se encuentra disperso a lo largo del dictamen del proyecto de Ley, por

lo que se sugiere ubicarlo en un solo capítulo ya que este tipo de derecho es para proteger los datos personales frente al tratamiento electrónico.

La protección de los derechos fundamentales en la red es cada día más necesaria. La sociedad de la información, basada cada vez en mayor medida en internet, posibilita que cualquier contenido (aún perjudicial, inexacto u obsoleto), pueda ser objeto de una divulgación desproporcionada, accediéndose al mismo casi de forma inmediata a través de distintas plataformas (como los buscadores o redes sociales).

En este árnbito el llamado "derecho al olvido", también denominado "derecho a vivir en paz", se ha convertido en una pieza clave para la defensa de las personas, ya sean anónimas o públicas.

La Directiva 95/46/CE del Parlamento Europeo y del Consejo del 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos, dispuso en sus artículos 6.1.c, 12 y 14, que los datos objeto de tratamiento **no podrían ser excesivos, debiendo suprimirse, rectificarse o bloquearse aquellos que fuesen inexactos o incompletos, y que a los particulares se les garantizaría la facultad para oponerse al tratamiento**. Esta directiva configuró el espíritu de lo que hoy se denomina "derecho al olvido".

No existía una regulación concreta del "derecho al olvido". Cierta parte de la doctrina ha venido usando dicho término para referirse a otros derechos específicos, recogidos en la Ley Orgánica Española 15/1999, de Protección de Datos de Personales, que se ejercitan para lograr la retirada o el bloqueo de datos personales generalmente en internet, o el cese de un determinado tratamiento, como por ejemplo el referido a la cancelación de antecedentes penales y policiales, así como la oposición a prácticas comerciales o publicitarias.

Respondiendo a la falta de regulación concreta, La Unión Europea elaboró un Reglamento relativo a la protección y circulación de datos personales, centrándose concretamente en el "derecho al olvido" y cabe esperar que esta nueva ordenación dote de mayor seguridad jurídica a los distintos operadores en lo referente a la protección de datos de carácter personal.

El "derecho al olvido" tiene, además, un innegable carácter transversal. No sólo puede constituir per se el objeto de un litigio, sino que su invocación y correcto ejercicio puede servir además, en todos los ámbitos jurisdiccionales y en procedimientos de distinta naturaleza, de fundamento para la adopción de medidas cautelares, cesación de las injerencias efectuadas y la reparación integral de los perjuicios sufridos.

No ocultamos que el "derecho al olvido" es ampliamente debatido, bien por los grandes operadores de internet (buscadores y redes sociales), bien por parte de la doctrina jurídica que afirma que no cabe hablar de "derecho al olvido", cuando aún no se contempla como tal en el ordenamiento jurídico el citado derecho. Sin embargo, el término "derecho al olvido" (con independencia de su regulación europea en materia de protección de datos) cabe aceptarse como una referencia comprensible de diferentes acciones jurídicas concretas, destinadas a proteger a las personas, generalmente, en la red.
Esta propuesta de redacción pretende hacer una recopilación de las principales normas referentes al llamado "derecho al olvido", teniendo en cuenta los diferentes ámbitos en los que se puede plantear.

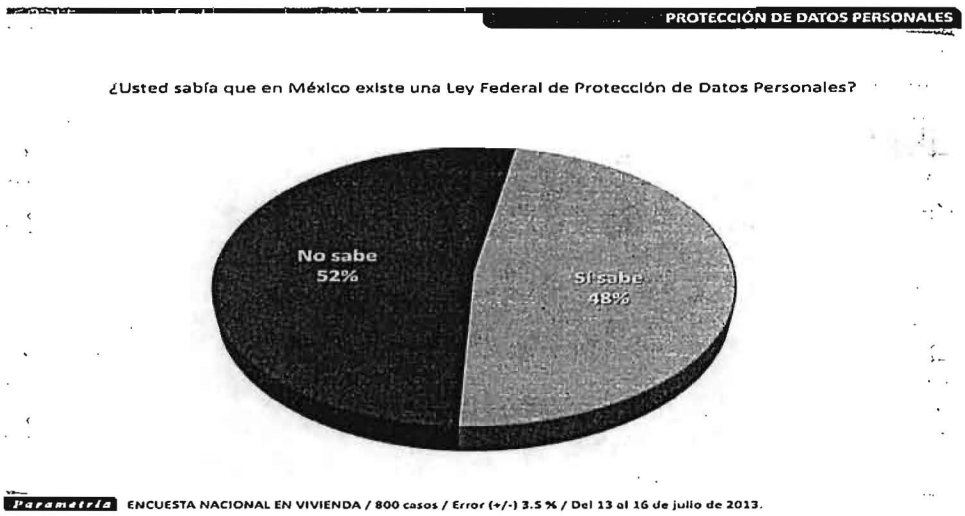
Por lo que se propone la siguiente redacción:

TITULO III **CAPÍTULO IV** **DEL DERECHO AL OLVIDO**
Artículo 58. El titular que vea afectada su reputación, tranquilidad personal, su moral y buena imagen, por el tratamiento electrónico de sus datos personales y que se encuentre sujeto a publicidad por medio de internet, podrá solicitar al responsable, en forma independiente de las acciones administrativas, civiles o penales que correspondan o incluso del derecho a la réplica, la cancelación y desindexación de sus datos personales.
Artículo 59. El derecho al olvido, no procederá en aquellos casos en dónde el interés de la sociedad sea mayor que el interés del titular de mantener esos datos personales excluidos del escrutinio público, como son las violaciones graves de derechos humanos, los delitos de lesa humanidad y los de alto impacto social. Para tal efecto, el responsable podrá solicitar una opinión técnica al Instituto, para que este en un plazo no mayor de cinco días hábiles decida la procedencia o no de la solicitud.
Artículo 60. El responsable no podrá alegar en contra del derecho al olvido ninguna de las excepciones contempladas en el artículo 55 de esta Ley para denegar su ejercicio. Únicamente se podrá limitar este derecho cuando el titular de los datos personales no compruebe que es mayor su interés de mantener su información de manera privada que el interés de la sociedad de conocerla; el responsable al emitir su respuesta deberá tomar como base los criterios de exactitud, relevancia pública y obsolescencia de los datos.
Para el ejercicio de este derecho, el titular deberá observar lo relativo al ejercicio de los derechos ARCO a que se refiere esta Ley, con relación al derecho de cancelación de datos personales, alegando por qué su interés de mantener su información de manera privada es mayor que el interés de la sociedad de conocerla. En la respuesta que emita, deberá de señalar las acciones que emprendió para la desindexación de los datos personales y el periodo que mantendrá bloqueado los datos.

7. En el **artículo 59** de la de ley, tomando en consideración que en muchas ocasiones los "encargados" serán personas físicas o morales y que se encuentran reguladas por la Ley Federal de Protección de Datos Personales en Posesión de los

Particulares, es que se propone imponer la obligación de los responsables se cercioré y obtenga la evidencia suficiente de que los encargados, en el caso de que así sea procedente, se encuentren alineados a la Ley antes citada.

Se busca incorporar esta obligación de manera expresa, en virtud, de que las estadísticas arrojadas en el 2013 por PARAMETRIA[1], sobre el conocimiento de la existencia de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, no ha variado mucho:



Es de destacar que, actualmente el INAI u otro organismo, cuenta con una estadística fiable, no sólo del nivel de cumplimiento de la citada Ley, sino el grado de calidad y profundidad de su adopción, ya que, nosotros sólo conocemos el 1% de las obligaciones ahí contempladas, que es el Aviso de Privacidad; de los cuales, los que me he detenido a revisar, no cumplen al 100% de los requisitos fijados por la Ley, su Reglamento o Lineamiento del Aviso de Privacidad.

DICE	DEBE DECIR
Artículo 59. La relación entre el responsable y el encargado deberá estar formalizada mediante contrato o cualquier otro instrumento jurídico que decida el responsable, de conformidad con la normativa que le resulte aplicable, y que permita acreditar su existencia, alcance y contenido.	**Artículo 59.** La relación entre el responsable y el encargado deberá estar formalizada mediante contrato o cualquier otro instrumento jurídico que decida el responsable, de conformidad con la normativa que le resulte aplicable, y que permita acreditar su existencia, alcance y contenido. **El encargado previo a la formalización de la relación, y en el caso de que se trate de un**

[1] Consultable en: http://www.parametria.com.mx/carta_parametrica.php?cp=4593

	sujeto obligado de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, deberá obtener la evidencia que considere necesaria para comprobar que se encuentre alineado a los lineamientos fijado por esa Ley.
En el contrato o instrumento jurídico que decida el responsable se deberá prever, al menos, las siguientes cláusulas generales relacionadas con los servicios que preste el encargado: ...	...

8. Uno de los puntos débiles que presenta la Ley, se encuentra precisamente en el Título Décimo Primero en donde se establecen las medidas de apremio y responsabilidades.
    - No se señalan las responsabilidades adrninistrativas.
    - El artículo 163 establece las causas de sanción por incumplimiento pero no señalan las responsabilidades económicas.

El **artículo 163** sólo señala en el **último párrafo** *"[l]as sanciones de carácter económico no podrán ser cubiertas con recursos públicos..."* lo que deja en un estado de incertidumbre tanto al servidor público que pudiera estar involucrado, así como al titular de los datos.

Lo anterior se debe a que en el artículo 164 se establece que quien conocerá y fijará la multa es el órgano de control interno; sin embargo para determinar la responsabilidad va en función al daño causado al erario público y no un daño de este tipo.

Ahora bien, con relación a las responsabilidades administrativas, civiles o penales que pueden derivar de ellas, y a pesar de que la lógica apunta que para su determinación se tendrá que aplicar las leyes de responsabilidades, las cuales no se encuentran homogenizadas al nivel de rigurosidad que impone la presente proyecto de ley; se propone incorporar de manera independiente las responsabilidades atribuibles a los servidores público que deriven de las leyes antes señaladas, diversas multas o sanciones monetarias, las cuales van desde las 100 hasta las 120,000 veces el valor diario de la Unidad de Medida y Actualización vigente, que serán cubiertas con el presupuesto del sujeto obligado, prohibiendo que estos soliciten ampliaciones presupuestales, a fin de dar cumplimiento a las señaladas multas. Lo anterior, con excepción de que con estas se ponga en riesgo la consecución de programas estratégicos, en materia de seguridad pública, nacional o salud. Las sanciones que

son propuestas, fueron diseñadas tomando como referencia la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, la cual, actualmente impone ese rango.

- La experiencia a nivel internacional, pero sobre todo en el país en relación con el robo, venta o filtración (tales como Liverpool y su padrón de clientes; Choice-point y recientemente por AMAZON MÉXICO del padrón electoral) de información personal, acceso indiscriminado a bases de datos personales o sencillamente el mal uso de estos general desconfianza para la población sobre la misma protección de datos personales; por lo que es necesario establecer sanciones económicas y los delitos en materia de tratamiento indebido de datos personales; esto siguiendo la lógica ya planteada por única Ley vigente a nivel federal del tema de protección de datos personales.

Artículo 169. Las infracciones a la presente Ley serán sancionadas por el Instituto con:
I. El apercibimiento para que el responsable actualice alguno de los supuestos contemplados en las fracciones V o VI del presente artículo;
II. Multa de 100 a 160,000 veces el valor diario de la Unidad de Medida y Actualización, en los casos previstos en las fracciones I, II, III, IV, XIV del presente artículo;
III. Multa de Multa de 200 a 320,000 veces el valor diario de la Unidad de Medida y Actualización, en los casos previsto en las fracciones VII a XIII del presente artículo.
Las anteriores sanciones económicas serán cubiertas con el presupuesto del sujeto obligado, y se harán efectivas por el Servicio de Administración Tributaria o las Secretarías de Finanzas u Órganos Electorales de las Entidades Federativas, según corresponda, a través de los procedimientos que las leyes establezcan, quien deberá enterar dichas multas al Instituto o los organismos garantes que corresponda, durante el periodo fiscal que se encuentre en curso.
El sujeto obligado no podrá solicitar ampliación presupuestal a fin de dar cumplimiento a las multas señaladas anteriormente, salvo que por su cobro, ponga en riesgo la consecución de programas estratégicos en materia de seguridad pública, seguridad nacional, o salud.

SUSCRIBE

Sen. Dolores Padierna Luna