OBLIGACIÓN DE NOTIFICAR A LA AUTORIDAD EN EL CASO DE VULNERACIONES DE SEGURIDAD EN MATERIA DE DATOS PERSONALES, DIFERENCIAS ENTRE LO PÚBLICO Y PRIVADO

Por Jonathan Mendoza Iserte
y Vitelio Ruiz Bernal

1. ANTECEDENTES

El derecho humano a la protección de datos personales se encuentra regulado en la Constitución Política de los Estados Unidos Mexicanos desde 2009. En aquel año se reformó el artículo décimo sexto y, consecuentemente, a partir de 2010, México cuenta con normatividad secundaria en materia de protección de datos personales en posesión de los particulares (sector privado).

Sin embargo, fue hasta el 7 de febrero de 2014, que se modifica el artículo sexto constitucional, dando pie a una reforma de gran calado y estableciendo en su régimen transitorio, la obligación de emitir legislación secundaria en materia de datos personales (dentro del año siguiente a dicha reforma), tanto para sector público como para sector privado.

Finalmente, casi tres años después, el 26 de enero de 2017, se publicó la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, que regula de forma directa al sector público federal y establece las bases y parámetros mínimos que deben atender las normativas locales en la materia. Con esto México se encontró en posibilidades de adherirse al Convenio 108 (Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981) del Consejo de Europa.

No obstante, no son pocos los que han dejado de considerar que el régimen transitorio de la reforma constitucional de 2014, también señalaba la necesidad de reformar la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, situación que hasta momento no ha acontecido.

Derivado de un trabajo de gestión por parte del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, la Cámara de Senadores del Honorable Congreso de la Unión aprobó el veintiséis de abril de dos mil dieciocho, la adhesión de México a el Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal y su protocolo adicional del Consejo de Europa; posteriormente, el instrumento de adhesión fue firmado por

el ejecutivo el diecinueve de junio de dos mil dieciocho, y depositado ante el Secretario General del Consejo de Europa, el veintiocho del propio mes y año, para finalmente ser publicado en el Diario Oficial de la Federación el veintiocho de septiembre de dos mil dieciocho marcando como fecha de su entrada en vigor el primero de octubre del mismo año

También conocido como "Convenio 108", su objetivo lo podemos visualizar en su artículo 1, que establece:

> *"Artículo 1 - Objeto y fin*
>
> *El fin del presente Convenio es garantizar en el territorio de cada Parte, a cualquier persona física, sean cuales fueren su nacionalidad o su residencia, el respeto a sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona ("protección de datos")."*[1]

Ciertamente, la adhesión al Convenio 108, implica un reconocimiento a los avances de México en la protección del derecho humano de la privacidad y la protección de datos personales, no obstante también genera un compromiso con la comunidad internacional que ineludiblemente debe implicar el avance para garantizar estos derechos humanos de cara a las nuevas realidades que se presenten.

En una primera aproximación, podríamos válidamente concluir que en estos diez años se ha visto un avance y compromiso por parte del Estado mexicano respecto a la tutela del derecho humano a la protección de datos personales, a la autodeterminación informativa. Sin embargo, si queremos seguir siendo un referente en Latinoamérica y garantizando este derecho humano es necesario, modificar y mejorar la normatividad, sobre todo la que respecto al ámbito de los particulares, es decir, el sector privado.

Bajo esta óptica, el presente análisis abordará uno de los temas que se estima trascendente en dos vertientes: i) la nacional, tanto para su armonización con la normativa con el sector público como para el avance en la protección efectiva de este derecho en el sector privado y; ii) la internacional, con la intención de generar condiciones más favorables para optar a la firma y adhesión del Protocolo 223 del Consejo de Europa, mejor conocido como *Convenio 108 Plus* e incluso ser candidatos para solicitar la adecuación normativa al nuevo Reglamento Europeo de Protección de Datos Personales, mismo que entró en vigor en mayo de 2018.

Como se mencionó previamente, uno de los temas trascendentales de reforma qué, desde nuestra perspectiva, resulta imperante impulsar normativamente en el sector

---

1 Diario Oficial de la Federación, *"Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, hecho en Estrasburgo, Francia, el veintiocho de enero de mil novecientos ochenta y uno."*, 28 de septiembre de 2018.

privado es la obligación de notificación a la autoridad de datos personales en caso de vulneraciones de seguridad en la materia. Vale la pena precisar que actualmente únicamente se tiene que dar aviso al titular de los datos.

Lo anterior, obedece a una consecuencia natural vinculada con el auge de las tecnologías de la información y comunicaciones (TIC), es decir, la adopción e implementación de las TIC de forma tan vertiginosa, en un sinfín de ámbitos y tareas que desarrolla el ser humano de forma cotidiana. Este uso intensivo de las TIC, también ha generado que alrededor de las mismas se encuentren errores, fallas e intentos de intervenir o acceder a ellas por la fuerza o sin autorización alguna, ya sea para tomar su control o para acceder a la información que se tiene almacenada, la cual, frecuentemente está compuesta por datos personales.

2. VULNERACIONES DE SEGURIDAD EN MATERIA DE DATOS PERSONALES

Concepto de Vulneración de Seguridad de Datos Personales

Para poder comprender la relevancia del tema en comento, es necesario en una primera instancia establecer que es una vulneración de seguridad en materia de datos personales y porque resulta tan relevante. Para lo anterior, tomaremos diversas definiciones, algunas doctrinales otras normativas tanto nacionales como internacionales.

Una violación de seguridad de datos personales es de acuerdo con el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares que establece en su artículo 63:

> "*Artículo 63. Las vulneraciones de seguridad de datos personales ocurridas en cualquier fase del tratamiento son:*
>
> I. *La pérdida o destrucción no autorizada;*
>
> II. *El robo, extravío o copia no autorizada;*
>
> III. *El uso, acceso o tratamiento no autorizado, o*
>
> IV. *El daño, la alteración o modificación no autorizada.*"[2]

Por su parte la Ley General de Protección de Datos Personales en Posesión de sujetos obligados establece en su artículo 38:

> *"Artículo 38. Además de las que señalen las leyes respectivas y la normatividad aplicable, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:*
>
> I. *La pérdida o destrucción no autorizada;*
>
> *II. El robo, extravío o copia no autorizada;*

2 Diario Oficial de la Federación, *"Ley Federal de Protección de Datos Personales en Posesión de los Particulares"*, 21 de diciembre de 2011.

III. El uso, acceso o tratamiento no autorizado, o

IV. El daño, la alteración o modificación no autorizada"3

Por su parte el Reglamento (UE) 2016/679 del Parlamento Europeo y Del Consejo, en su artículo 4, apartado 12 establece:

> *"Artículo 4*
>
> *Definiciones*
>
> *A efectos del presente Reglamento se entenderá por:*
>
> *...*
>
> *12) «violación de la seguridad de los datos personales»: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;*
>
> *..."*[4]

De las tres definiciones normativas anteriores podemos desprender que una violación o vulneración de la seguridad de los datos personales es cualquier acción que implique la destrucción, perdida, alteración accidental o ilícita, el robo, el extravío, copia no autorizada, el acceso no autorizado, el daño y la comunicación no autorizada en cualquier fase del tratamiento de datos personales.

Precisiones y Análisis del Concepto de Vulneración de Seguridad de Datos Personales

El Grupo de Trabajo Sobre Protección de Datos del Artículo 29, en sus "*Directrices sobre la notificación de violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679"*[5] realiza diversas precisiones que se estima pertinente analizar con respecto al concepto de violación de seguridad de los datos personales.

Dentro de las precisiones que analiza y realiza el grupo de trabajo del artículo 29, respecto de los componentes del concepto de violación de seguridad se encuentran:

- La "destrucción", la misma se da cuando los datos ya no existen, o ya no existen en una forma que sea de utilidad para el responsable del tratamiento.

---

3 Diario Oficial de la Federación, *"Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados"*, 26 de enero de 2017.

4 Diario Oficial de la Unión Europea, "*REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO*", 27 de abril de 2016.

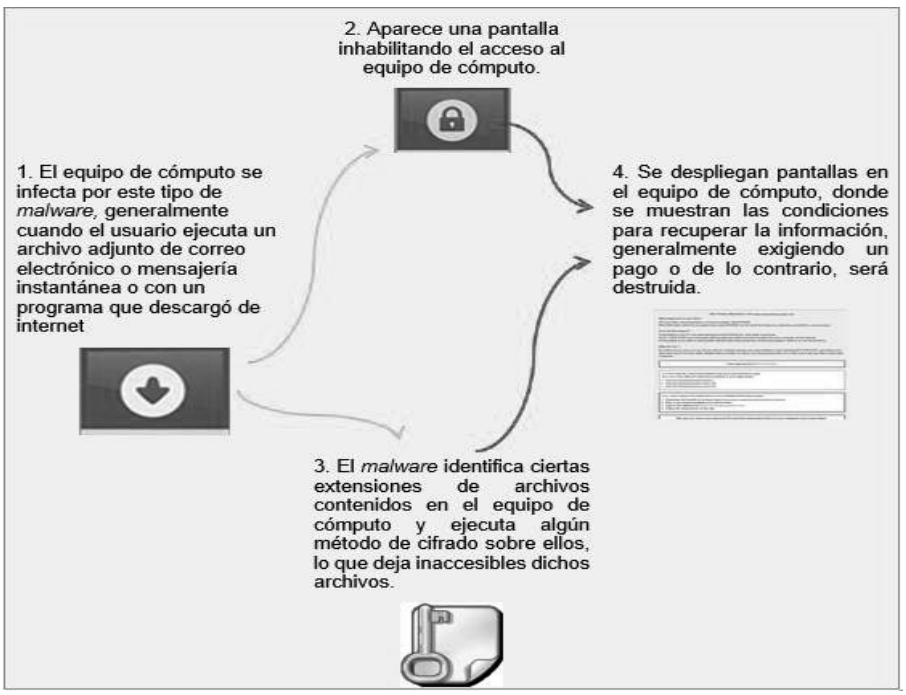
5 Grupo de Trabajo Sobre Protección de Datos del Artículo 29, "*Directrices sobre la notificación de violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679,* https://www.aepd.es/media/criterios/wp250rev01-es.pdf, el 25 de abril de 2019.

– El "daño" se da cuando los datos han sido alterados, corrompidos o dejan de estar completo.

– La "pérdida" se da cuando los datos siguen existiendo, pero el responsable del tratamiento ha perdido el control sobre ellos o el acceso o ya no obran en su poder.

– El "acceso no autorizado", que puede incluir la divulgación de los mismos, o el acceso a destinatarios que no están autorizados para recibir o acceder a los datos o cualquier forma de tratamiento.

Ahora bien, de lo que se tiene certeza es que una vulneración es un incidente de seguridad, pero no todo incidente de seguridad es una vulneración de datos personales, por ejemplo, algunos ransomware como wanna cry (programa malicioso que cifra la información de una computadora, de manera que el usuario pierde el acceso a sus archivos, y para recuperarlos debe pagar un rescate, sin que exista la garantía de que se recupere la información).



Contrario a este esquema, una vulneración de seguridad que necesariamente implique la obtención ilegal de información puede comprometer datos personales. En este escenario la consecuencia lógica, es que el responsable se ve imposibilitado en cumplir adecuadamente con los principios y deberes establecidos en las diversas normativas de protección de datos personales. Lo anterior, no necesariamente significa que dicha

vulneración sea imputable al responsable. Precisamente para determinar o delimitar el nivel de responsabilidad resulta indispensable regular en sector privado, la obligación de notificar a la autoridad de dicho incidente.

Tipos de Vulneraciones de Seguridad

Para poder comprender cuales son las implicaciones de las vulneraciones de seguridad, es necesario categorizar las mismas, en ese sentido el grupo de trabajo del artículo 29 propuso desde su opinión 03/2014, tres categorías de vulneraciones de seguridad o violaciones de seguridad en datos personales a saber:

- Violación de confidencialidad, la misma se da cuando se revela o de divulga datos personales de forma accidental o intencional, o se da un acceso no autorizado a los mismos.
- Violación de integridad, cuando se produce una alteración no autorizada o accidental de los datos personales.
- Violación de disponibilidad, cuando se da una perdida de acceso a los datos personales de forma accidental o no autorizada[6]

Es importante precisar que una vulneración de seguridad puede afectar la confidencialidad, la integridad y la disponibilidad de los datos personales de forma simultánea, o en alguna combinación de cualquier de los tipos antes mencionados.

Vale la pena mencionar que mientras una vulneración de seguridad de los tipos relacionados con la integridad o la confidencialidad pueden resultar evidentes, en el caso de las vulneraciones de disponibilidad los casos pueden resultar menos evidentes.

Consecuencias de las vulneraciones de Seguridad

Ahora bien, las vulneraciones de seguridad de datos personales cobran relevancia no solo en sentido de la utilidad y el tratamiento necesario que realiza el responsable, sino que además resulta de una importancia aun superior para el caso de los titulares, es decir las afectaciones que podría sufrir un titular de los datos personales, con respecto a una vulneración de seguridad, puede inferirle graves daños e inclusive podría poner en peligro su vida.

Lo anterior es así, ya que en el momento en que se genera una vulneración de seguridad y datos personales dentro de los efectos inmediatos, se encuentra que le titu-

6 Grupo de Trabajo Sobre Protección de Datos del Artículo 29, "*Directrices sobre la notificación de violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679,* https://www.aepd.es/media/criterios/wp250rev01-es.pdf, el 25 de abril de 2019.

lar pierde el control sobre sus datos personales y de facto existe una restricción a su derecho, en el mismo sentido existe un riesgo latente dependiendo del tipo de datos personales que se hubieren visto afectados por la vulneración de que el titular de los mismos y en razón de dicho incidente sufra discriminación, robo de identidad, fraude, pérdidas financieras, la reversión de procesos de *pseudonimización* que permitan la inferencia o conocimiento de otros datos que no se encontraban expuestos, así como, la perdida de la confidencialidad de los mismos.

Es decir, el sólo hecho de la pérdida o divulgación de los datos personales de un titular a consecuencia de una vulneración de seguridad puede implicar una serie de consecuencias inimaginables mismas que se pueden materializar en hechos que no solo afectan la esfera jurídica de su titular, sino que le afectan en situaciones de hecho no solo derecho.

Este tipo de vulneraciones que tienen implicaciones de hecho y derecho para los titulares de los datos, constituye el motivo principal para colegir que es fundamental normar la obligación de notificación de vulneraciones de seguridad en una doble dimensión es decir no sólo basta que se notifique al titular de los datos o a la autoridad de la materia, sino que se debe de realizar de forma simultánea a ambos actores, a efecto de uno pueda tomar las medidas que estima pertinentes a efecto de salvaguardar su vida, patrimonio e intereses; y el otro pueda supervisar y verificar que la situación se contenga y mitigue por parte del Responsable, así como asegurar que la misma no vuelva a suceder. [7]

3. NOTIFICACIÓN DE VULNERACIONES DE SEGURIDAD

Notificación de Vulneraciones de Seguridad en el Derecho Nacional

Notificaciones de Vulneraciones de Seguridad en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Como se mencionó en párrafos anteriores, en México no existe una sola fuente normativa por lo que respecta a la materia de datos personales, en primera instancia y por orden cronológico se tiene la Ley Federal de Protección de Datos Personales en Posesión de los Particulares misma que fue publicada en el Diario Oficial de la Federación en 2010, su ámbito de aplicación corresponde al orden federal y regula a todos los particulares que lleven a cabo el tratamiento de datos personales, la autoridad competente es del orden nacional en este caso corresponde al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Es conveniente mencionar que esta ley y su reglamento, fueron inspirados, en una buena medida, en el modelo

7 Grupo de Trabajo Sobre Protección de Datos del Artículo 29, "*Directrices sobre la notificación de violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679,* https://www.aepd.es/media/criterios/wp250rev01-es.pdf, el 25 de abril de 2019.

europeo y en consecuencia abreva muchos de sus contenidos de la hoy derogada directiva 95/46.

Por lo que respecta a la notificación de vulneraciones de seguridad, la ley en comento, contempla en su artículo 20 lo siguiente:

> *"Artículo 20.- Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este* último *pueda tomar las medidas correspondientes a la defensa de sus derechos."*[8]

De una primera lectura podemos notar que, de ocurrir una vulneración de seguridad en cualquier fase del tratamiento, cuando se afecten de forma significativa los derechos patrimoniales o morales de los titulares se deberán notificar **únicamente** por el responsable a los titulares de los datos personales.

La normativa actual para el caso de los particulares, no contempla una notificación a la autoridad de la materia, en el mismo sentido, nos encontramos ante una norma imperfecta es decir por un lado la propia redacción del artículo deja elementos dentro del mismo que pueden ser objeto de diversas interpretaciones. Dentro los elementos que son interpretables encontramos el adverbio "inmediatamente"; si bien la Real Academia de la Lengua Española establece su significado como "sin interposición de otra cosa, "ahora, al punto, al instante"[9]; se estima que el mismo, al no establecer un reflejar un plazo específico, genera discrecionalidad y, consecuentemente la notificación al titular, en la práctica podría no darse de la forma más adecuada.

Por otro lado, la frase "que afecte de forma significativa" se encuentra sujeta a interpretación también, ya que al no participar la autoridad como parte de la notificación queda a juicio del responsable el establecer que se entiende por "de forma significativa" lo que de nueva cuenta pudiera no estar alineado con la tutela efectiva del derecho de protección de datos personales de los titulares.

Finalmente desde un aspecto distinto a la técnica legislativa, vinculado con los efectos de la norma, continua siendo una supuesto jurídico imperfecto, toda vez que la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, no contempla una sanción concreta para aquellos casos en que el Responsable sea omiso respecto de las notificaciones de vulneraciones de seguridad de datos personales a los titulares, por lo que la autoridad sólo podría imponer una sanción, a través de resoluciones que argumenten la violación al principio de responsabilidad, o en su caso, al deber de se-

---

8 Diario Oficial de la Federación, *"Ley Federal de Protección de Datos Personales en Posesión de los Particulares"*, 21 de diciembre de 2011.

9 Real Academia de la Lengua Española, *Inmediatamente, consultado en:* http://lema.rae.es/drae2001/srv/search?id=mD9CwP3yHDXX25HbD1Eh, consultado el 25 de mayo de 2019.

guridad; claro siempre que la autoridad llegue a tener conocimiento de la vulneración de seguridad de datos personales.

Notificaciones de Vulneraciones de Seguridad en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Su nombre lo establece, nos encontramos ante una norma general, que es de aplicación directa para la Federación, continuando con la misma lógica, las entidades federativas regulan dentro del ámbito de sus competencias la materia, con la obligación de apegarse a los preceptos establecidos en la ley marco, por lo que para efectos de este breve análisis nos limitaremos a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, sin dejar de reconocer la existencia de la normativa que los Congresos locales han emitido en la materia.

Dicho lo anterior, el ámbito de aplicación de esta norma se encuentra circunscrito a los tres niveles de gobierno (ámbitos federal, estatal y municipal), respecto de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos; tal como lo establece el su artículo primero. Es decir, en general a cualquier autoridad, de cualquier nivel de gobierno y de cualquier poder que constitucionalmente se encuentre reconocido.

Como se ha mencionado en párrafos anteriores, desde los inicios de la regulación en la materia de datos personales, México se ha inclinado para incorporar a su cuerpo normativo el modelo europeo, el caso de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, no se la excepción. Esta norma tiene su génesis en las reformas constituciones en materia de transparencia y protección de datos personales de 2014, no obstante, dicha normativa fue publicada hasta enero de 2017. Se precisa que leales a los antecedentes y a los modelos que se habían adoptado en la materia, el legislador tomó como una de las fuentes más relevantes al nuevo y en aquel entonces aún no vigente "Reglamento (UE) 2016/679 del Parlamento Europeo y Del Consejo", mejor conocido como RGPD, reglamento que derogó la directiva 95/46, respecto de esta normativa nos referiremos más adelante.

Ahora bien, respecto de las notificaciones de vulneraciones de seguridad encontramos en esta normativa las siguientes disposiciones:

> *"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 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.*

Articulo 41. El responsable deberá informar al titular al menos lo siguiente:

I. La naturaleza del incidente;

II. Los datos personales comprometidos;

III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;

IV. Las acciones correctivas realizadas de forma inmediata, y

V. Los medios donde puede obtener más información al respecto.

...".[10]

De la lectura de los preceptos citados, podemos notar que este aspecto, como en algunos más que no son materia de este estudio (***vg.*** *datos personales de personas fallecidas, portabilidad*), existe una evidente evolución normativa entre la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

La normativa de sujetos obligados, incorpora la obligación de notificar tanto a la autoridad competente como a los titulares de los datos, en el mismo sentido pretende establecer una regla de temporalidad, indicando que sin dilación alguna, el momento oportuno para realizarla es a partir que se tenga confirmación que existió la vulneración y que el responsable ha iniciado un proceso de revisión exhaustivo a efecto de conocer la magnitud de la misma; esto con el objetivo de que los titulares puedan tomar las medidas que estimen pertinentes para la defensa de sus derechos.

Asimismo, el artículo 41 señala que elementos deben integrarse a las notificaciones que se realicen a los titulares, por ejemplo, se deberá describir la naturaleza del incidente, cuáles son los datos personales comprometidos, qué medidas puede adoptar el titular para retomar sus intereses, cuáles son las acciones correctivas que el responsable ha tomado de forma inmediata y los medios por los que puede obtener más información al respecto.

Se precisa que el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares ya recogía disposiciones normativas con una redacción semejante, con la diferencia que la notificación de la vulneración sólo se encuentra prevista para el titular de los datos personales.

Finalmente, se estima que existe un avance con respecto de la normativa para los particulares, no obstante ello, continúan algunas imprecisiones tales como la frase que "afecten de manera significativa", lo cual fue comentado párrafos anteriores; si bien con la notificación a la autoridad se podrían subsanar muchas de las imprecisiones es necesario que la autoridad desarrolle metodologías que permitan establecer que se

10 Diario Oficial de la Federación, *"Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados"*, 26 de enero de 2017.

entiende por afectaciones de manera significativa, en el mismo sentido, como se había mencionado anteriormente, existe una falta de precisión de los plazos; para el caso de la federación dicha imprecisión fue subsanada por el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, a través de la expedición y publicación del Acuerdo mediante el cual se aprueban, los lineamientos federales de protección de datos personales para el sector público, en los cuales encontramos las siguientes disposiciones normativas:

> *"...*
>
> *Artículo 66. De conformidad con lo dispuesto en el articulo 40 de la Ley General, el responsable deberá notificar al titular y al Instituto las vulneraciones de seguridad que de forma significativa afecten los derechos patrimoniales o morales del titular dentro en un plazo máximo de setenta y dos horas, a partir de que confirme la ocurrencia de éstas y el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de mitigación de la afectación.*
>
> *El plazo a que se refiere el párrafo anterior, comenzará a correr el mismo día natural en que el responsable confirme la vulneración de seguridad.*
>
> *Para efectos del presente articulo, se entenderá que se afectan los derechos patrimoniales del titular cuando la vulneración esté relacionada, de manera enunciativa más no limitativa, con sus bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados o las cantidades o porcentajes relacionados con la situación económica del titular.*
>
> *Para los efectos del presente artículo, se entenderá que se afectan los derechos morales del titular cuando la vulneración esté relacionada, de manera enunciativa más no limitativa, con sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspecto físicos, consideración que de sí mismo tienen los demás, o cuando se menoscabe ilegítimamente la libertad o la integridad física o psíquica de* éste.
>
> *Artículo 67. En la notificación a que se refiere el artículo anterior, el responsable deberá informar mediante escrito presentado en el domicilio del Instituto, o bien, a través de cualquier otro medio que se habilite para tal efecto, al menos, lo siguiente:*
>
> *I. La hora y fecha de la identificación de la vulneración;*
>
> *II. La hora y fecha del inicio de la investigación sobre la vulneración;*
>
> *III. La naturaleza del incidente o vulneración ocurrida;*
>
> *IV. La descripción detallada de las circunstancias en torno a la vulneración ocurrida;*
>
> *V. Las categorías y número aproximado de titulares afectados;*
>
> *VI. Los sistemas de tratamiento y datos personales comprometidos;*
>
> *VII. Las acciones correctivas realizadas de forma inmediata;*
>
> *VIII. La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida;*
>
> *IX. Las recomendaciones dirigidas al titular;*

X. El medio puesto a disposición del titular para que pueda obtener mayor información al respecto;

XI. El nombre completo de la o las personas designadas y sus datos de contacto, para que puedan proporcionar mayor información al Instituto, en caso de requerirse, y

XII. otra información y documentación que considere conveniente hacer del conocimiento del Instituto.

Artículo 68. En la notificación que realice el responsable al titular sobre las vulneraciones de seguridad a que se refieren los artículos 40 de la Ley General y 66 de los presentes Lineamientos generales deberá informar, al menos, lo siguiente:

I. La naturaleza del incidente o vulneración ocurrida;

II. Los datos personales comprometidos;

III. Las recomendaciones dirigidas al titular sobre las medidas que éste pueda adoptar para proteger sus intereses;

IV. Las acciones correctivas realizadas de forma inmediata;

V. Los medios puestos a disposición del titular para que pueda obtener mayor información al respecto;

VI. La descripción de las circunstancias generales en torno a la vulneración ocurrida, que ayuden al titular a entender el impacto del incidente, y

VII. Cualquier otra información y documentación que considere conveniente para apoyar a los titulares.

El responsable deberá notificar directamente al titular la información a que se refieren las fracciones anteriores a través de los medios que establezca para tal fin. Para seleccionar y definir los medios de comunicación, el responsable deberá considerar el perfil de los titulares, la forma en que mantiene contacto o comunicación con éstos, que sean gratuitos; de fácil acceso; con la mayor cobertura posible y que estén debidamente habilitados y disponibles en todo momento para el titular.

Articulo 69. En términos de lo previsto en los artículos 40 de la Ley General y 66 de los presentes Lineamientos generales, una vez que le sea notificada una vulneración de seguridad, el Instituto deberá realizar las investigaciones previas a que hubiere lugar con la finalidad de allegarse de elementos que le permitan, en su caso, valorar el inicio de un procedimiento de verificación conforme a lo dispuesto en la Ley General y los presentes Lineamientos generales.

...".[11]

De los artículos anteriores podemos concluir que los mismos cubren las deficiencias legislativas, que hemos comentado en la primera parte de este análisis, con respecto a la frase de "forma significativa" y las precisiones de los plazos, al establecer el plazo de 72 horas contado a partir de la confirmación de la vulneración. Incluso establece

11 Diario Oficial de la Federación, "*ACUERDO mediante el cual se aprueban los Lineamientos Generales de Protección de Datos Personales para el Sector Público*", 26 de enero de 2018.

requisitos más rigurosos con relación a los contenidos de las notificaciones tanto de los titulares como a la autoridad, lo que permite precisamente brindar certeza por lo que refiere a los términos de las vulneraciones de seguridad.

Consideraciones en torno a las leyes de protección de datos personales en posesión de los particulares y de sujetos obligados

Del análisis de la legislación nacional podemos concluir válidamente que, tenemos dos normativas que convergen en los principios y conceptos que permiten garantizar el derecho a la protección de datos personales; no obstante ello, advertimos asimetrías en dichas normativas, causadas principalmente por el lapso de tiempo transcurrido entre la emisión de la primera en 2010 (sector privado) y la segunda en 2017 (sector público); la diferencia de más de 5 años entre la dos, ha generado distorsiones respecto de la forma en que se garantiza este derecho humano.

La normatividad de datos personales en posesión de los particulares necesita homologarse a las nuevas exigencias y obligaciones contempladas en la ley de sujetos obligados, no solo porque el derecho en el ámbito privado debe evolucionar a las nuevas realidades que enfrenta en el país, sino porque se debe buscar la tutela efectiva e integral del derecho humano a la protección de los datos personales de los mexicanos, situación que no se logra a cabalidad con las asimetrías que actualmente encontramos en estas normativas.

Notificaciones de violaciones de seguridad en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo

A lo largo de este estudio hemos hecho referencias al derecho europeo, y de cómo la normatividad en México ha adoptado varios elementos del modelo de protección de datos personales de dicha región. Por lo anterior, se estima pertinente mencionar como es que se encuentra normado las notificaciones de las "vulneraciones de seguridad" para el derecho mexicano o "violaciones de seguridad" para el derecho europeo.

El Reglamento (UE) 2016/679 del Parlamento Europeo y Del Consejo, mejor conocido como Reglamento de Protección de Datos Personales (RPGD), establece las siguientes disposiciones al respecto:

> *"...*
>
> *Artículo 33*
>
> *Notificación de una violación de la seguridad de los datos personales a la autoridad de control*
>
> *1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que*

dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, debera ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 debera, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;

c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;

d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitira a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo.

Artículo 34

Comunicación de una violación de la seguridad de los datos personales al interesado

1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;

c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podra exigirle que lo haga o *podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3…".*[12]

De la normativa anterior, se advierte que por lo que respecta a las notificaciones de violaciones, algunos autores señalan como un elemento novedoso del reglamento, el hecho que si no se toman a tiempo las medidas adecuadas, estas violaciones pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, tales cómo la perdida de control sobre su datos personales o las restricción de sus derechos. [13]

Dicho lo anterior, también de un breve análisis se pueden encontrar algunas diferencias importantes con respecto a la notificación de vulneraciones de seguridad en materia de datos personales para sujetos obligados de la normatividad mexicana. Dentro de estas divergencias destacan las excepciones a las notificaciones de los titulares siempre y cuando se cumplan supuestos específicos. La facultad establecida de las autoridades de control para ordenar la notificación por así estimarlo conveniente.

En el mismo sentido, por lo que hace a la notificación de las autoridades de control, es decir en las mismas también existe una excepción para la notificación de la autoridad del control, y se establecen conceptos respecto de los plazos y la dilación de la notificación, así como la justificación de la misma; también incluye la capacidad de proveer la información relacionada con la violación de seguridad de forma paulatina en lugar que se entregue de forma simultánea.

Se desprende de la lectura de estos preceptos normativos, que los mismos fueron desarrollados por el legislador europeo tratando de adoptar elementos que permitan a dicha normativa adaptarse a la realidad, es decir, pareciera que los mismos se encuentran redactados para aun aplicación práctica y casi a forma de instructivo paso a paso, situación que evidentemente facilita la puesta en práctica de estas notificaciones.

---

12 Diario oficial de la Unión Europea; *"Reglamento (UE) 2016/679 del Parlamento Europeo y Del Consejo"*, 27 de abril de 2016.

13 Arias Pou María, "VIII. Definciones a Efectos del Reglamento General de Protección de Datos" en: Piñar Mañas José Luis, María Álvarez Caro y Miguel Recio Gayo (comps): "Reglamento General de Protección de Datos Personales – Hacia un nuevo modelo europeo de privacidad", Madrid, España, Reus, 2016, p. 129.

4. CASOS PRÁCTICOS

Se busca ejemplificar con algunos asuntos las diferencias manifiestas entre las normativas de datos personales por un lado La Ley Federal de Protección de Datos Personales en Posesión de los Particulares y por el otro le Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; como se ha mencionado en párrafos anteriores, la diferencia en la notificación de vulneraciones de seguridad entre una ley y la otra radica esencialmente en la obligatoriedad de la ley de sujetos obligados de notificar a la autoridad competente.

Notificación de vulneraciones de seguridad en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

En enero de 2019 en la red social Twitter, un usuario con conocimientos de informativa y ciberseguridad, señaló que, había encontrado la información relativa a (4,072,738 documentos) correspondiente a diversos comprobantes de nómina de diferentes compañías.

Los primeros días de febrero de 2019, se recibió correo electrónico por parte de dicho usuario en el que esencialmente mencionaba:

A finales de enero de 2019, había identificado una base de datos de MongoDB sin contraseña con casi 5 millones de registros etiquetados como CFDI (abreviatura de Comprobantes Fiscal Digital por Internet), el esquema de facturación electrónica definido por el código fiscal federal mexicano.

[...]

La base de datos estaba compuesta con varios gigabytes de información y contenía numerosas colecciones que llevan el nombre de la identificación fiscal de México de una compañía.

Cada colección tenía un número diferente de documentos (el más grande tenía alrededor de 6K documentos), con toda la información que esperaría de la base de datos de cuentas electrónicas.

Algunas facturas eran documentos de nómina, con datos personales de personas físicas en los cuales se incluyen los siguientes datos personales: CURP, números de seguridad social nacional, tasa salarial etc.

Después de casi 48 horas de estar expuesta a la Internet pública, la base de datos había sido secuestrada, se dejó una nota de rescate que exigía que 0.5 BTC a cambio de devolver los datos.

A finales de febrero de 2019, se recibió un correo electrónico del mismo usuario de Twitter en el cual precisó que recibió una copia anónima de un documento que con-

firma que una firma de consultoría se comunica con las empresas que se encontraban listadas en la base de datos antes mencionada y asume la responsabilidad de la vulneración de seguridad de datos personales.

Por lo anterior, el a finales de febrero de 2019, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, emitió acuerdo de inicio de oficio de procedimiento de investigación en contra de la firma de consultoría.

Si bien la investigación aún se encuentra sustanciándose en el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, lo que podemos concluir de los hechos antes mencionados, es que en materia de particulares la autoridad sólo tiene las facultades de iniciar procedimientos de investigación o verificación de oficio si elementos que le permitan de manera fundada y motivada presumir violaciones a la normatividad en la materia, lo cual limita de forma importante el actuar del mencionado Instituto. En el mismo sentido, derivado de la falta de marco normativo que obligue a los particulares a dar notificación al Instituto, es que de forma frecuente el Instituto no tiene forma de allegarse de forma oportuna de los elementos que le permitirán iniciar las investigaciones de oficio derivadas de vulneraciones de seguridad en materia de datos personales.

Notificación de vulneraciones de seguridad en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Según diversas notas periodísticas publicadas en abril de 2019, así como de un usuario de la red social Twitter; se habrían publicado presuntamente datos personales en posesión de la una oficina de una dependencia del gobierno federal. Sin que se contarán con los elementos probatorios suficientes para confirmar por cuenta propia los hechos narrados en los medios noticiosos.

Dicha dependencia del gobierno federal emitió un comunicado en el que informa en esencia que se detectaron fallos técnicos (mismos que ya se habían corregido) que permitieron una vulneración en un equipo que se encuentra en una de las oficinas de dicha dependencia.

A su vez, mencionaron que la información que se había comprometido se limitaba a un número pequeño de titulares y que sus sistemas generales de información no se habían visto comprometidos de forma alguna.

La dependencia del gobierno federal debió por obligación legal remitir al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales una notificación con respecto a la vulneración de seguridad consistente en la extracción de información de un equipo de cómputo que se encontraba en una de sus oficinas con lo cual se comprometieron datos personales. Lo cierto es que no existe certeza o no de que la misma se hubiese realizado hasta el momento.

Tras la supuesta notificación el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, debería de iniciar de oficio un procedimiento de investigación por presuntas violaciones a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En efecto, en México nos encontramos frente a una novedad normativa, tras la ya no tan reciente publicación y entrada en vigor de una ley de protección de datos personales para el sector público (2017).

En este sentido, aun cuando el Instituto no se enteró de primera cuenta de la vulneración, la multiplicidad de indicios con que se contaban con respecto de los hechos narrados por los medios de comunicación, así como por los usuarios de redes sociales son suficientes para detonar una investigación de oficio por parte de la autoridad competente.

Ello, aunado a la obligación que la normativa impone a los sujetos obligados de los tres niveles de gobierno de notificar a la autoridad competente con respecto de las vulneraciones de seguridad que sufran.

Por lo anteriormente expuesto, consideramos que en ámbito (sector público) se da un nivel de protección más adecuado e integral respecto de los datos personales, en lo que atañe a posibles violaciones al principio de responsabilidad y el deber de seguridad.

En el mismo sentido, estas notificaciones permiten que las autoridades competentes actúen, de forma mucho más expedita, lo que se traduce en: denotar o implementar mecanismos para aminorar las afectaciones que puedan sufrir los titulares de los datos, allegarse de mejores elementos probatorios o de elementos probatorios idóneos, los cuales se pueden perder con el sólo paso del tiempo y sustanciar procedimientos de investigación que de no tener las notificaciones adecuadas hubieran sido imposibles de iniciar.

5. CONCLUSIONES

Las vulneraciones o violaciones de seguridad en materia de datos personales no son algo novedoso ni para la legislación mexicana, ni para la europea, no obstante, se ha establecido que dicha obligación a evolucionado de forma positiva y en un contexto que busca mejorar el derecho a la autodeterminación informativa.

Si bien, México podemos decir es referente en datos personales a nivel Latinoamérica, actualmente tiene una dicotomía en cómo se garantiza el derecho a la protección de los datos personales, es decir los titulares son los mismos, pero el nivel de protección dependerá de quien es el responsable del tratamiento de datos personales si el mismo pertenece al sector público o al sector privado.

Lo anterior, genera inevitablemente asimetrías o distorsiones en la tutela del derecho humano de protección de los datos personales, lo que se convierte en una necesidad conveniente y en algunos casos urgente de homologar la normativa de datos personales en posesión de los particulares con la normativa de sujetos obligados. Quizá recogiendo las mejores prácticas que ha adoptado en el Reglamento General de Protección de Datos Personales, a efecto de facilitar una implementación sencilla de estas nuevas obligaciones.

6. FUENTES DE CONSULTA

Diario Oficial de la Federación, *"Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, hecho en Estrasburgo, Francia, el veintiocho de enero de mil novecientos ochenta y uno."*, 28 de septiembre de 2018.

Diario Oficial de la Federación, *"Ley Federal de Protección de Datos Personales en Posesión de los Particulares"*, 21 de diciembre de 2011.

Diario Oficial de la Federación, *"Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados"*, 26 de enero de 2017.

Diario Oficial de la Unión Europea, "*REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO*", 27 de abril de 2016.

Grupo de Trabajo Sobre Protección de Datos del Artículo 29, "*Directrices sobre la notificación de violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679,* https://www.aepd.es/media/criterios/wp250rev01-es.pdf, el 25 de abril de 2019.

Diario Oficial de la Federación, "*ACUERDO mediante el cual se aprueban los Lineamientos Generales de Protección de Datos Personales para el Sector Público*", 26 de enero de 2018.

Diario oficial de la Unión Europea; *"Reglamento (UE) 2016/679 del Parlamento Europeo y Del Consejo"*, 27 de abril de 2016.

Arias Pou María, "VIII. Definiciones a Efectos del Reglamento General de Protección de Datos" en: Piñar Mañas José Luis María Álvarez Caro y Miguel Recio Gayo (comps): "Reglamento General de Protección de Datos Personales – Hacia un nuevo modelo europeo