Compliance digital

La rama del *compliance* ignorada por todos los expertos

El *compliance* se ha convertido en un sector fundamental para el desarrollo de los abogados de empresa. Sin embargo, esta rama suele ceñirse a ciertos rubros como anticorrupción, prevención de *lavado* de dinero y responsabilidad penal de las empresas, dejando fuera otros apartados igual de importantes. En este artículo analizaremos el *compliance* digital

Autor: Joel Alejandro Gómez Treviño, Coordinador del Comité de Derecho de las Tecnologías de la Información y Protección de Datos Personales de Asociación Nacional de Abogados de Empresa, Colegio de Abogados

INTRODUCCIÓN

No podemos negar que México es un país de modas. Temas como *compliance*, protección de datos personales, prevención de *lavado* de dinero, *Fintech* y *Legaltech*, entre otros, son temas que desde hace algunos años están de moda. Eso significa, no sólo que hay una considerable oferta de cursos, congresos y conferencias sobre estos temas, sino también que existe un *tsunami* de expertos en cada materia.

Estas *modas* para la abogacía usualmente obedecen a cambios en el entorno regulatorio o a tendencias en el ámbito normativo de negocios provenientes del extranjero.

¿ES EL COMPLIANCE UNA MODA O UN DOGMA DE FE?

El *compliance* es una moda por varias razones, principalmente por la gran oferta de capacitación y publicaciones que abordan esta materia. Tan es un tema de moda, que nos empeñamos en seguirle llamando *compliance*, cuando técnicamente podríamos traducirlo como "cumplimiento".

Además, no se puede ignorar que hasta hace cinco años, o un poco más, los abogados dominábamos el ámbito legal en las empresas bajo el nombre de "departamento jurídico" o "dirección legal".

Hoy en día, existe una bifurcación de funciones, pues muchas empresas, además de tener el departamento jurídico tienen otro, al que suelen llamar "gerencia regulatoria" o incluso "departamento –u oficial– de cumplimiento". En ocasiones esta área depende de la dirección jurídica, pero cada vez se ve con mayor frecuencia que esta posición ya ha adquirido otra tan dominante en algunas empresas, que incluso crean una dirección o departamento independiente de cumplimiento.

Por otro lado, muchas personas están acostumbradas a que si escuchan lo mismo muchas veces, lo toman como dogma de fe, aceptando y creyendo en ello de manera irrevocable. De acuerdo con Henry Vargas Holguín, en la Iglesia católica un "dogma" es una verdad de fe infalible, incuestionable, absoluta, definitiva, inmutable y segura, sobre la cual no puede subsistir ninguna duda.

Por ahora, sin temor a equivocarme, puedo afirmar que el tema de cumplimiento no sólo es una moda sino también un dogma de fe. Más adelante explicaré las razones que me llevan a concluir esto último.

¿QUÉ ES COMPLIANCE?

Desde un punto de vista meramente gramático, el Diccionario de Cambridge define a *compliance* como...

> *el acto de obedecer una orden, regla o solicitud.*

Para el *Diccionario Merriam-Webster*, significa:

> *...el acto o proceso de cumplir un deseo, demanda, propuesta, régimen o coacción. Conformidad en el cumplimiento de los requisitos oficiales.*

El *Diccionario de Negocios* va un poco más allá, al definir este término como:

> *Certificación o confirmación de que el autor de una acción (como el autor de un informe de auditoría), o el fabricante o proveedor de un producto, cumple con los requisitos de las prácticas aceptadas, la legislación, las normas y regulaciones prescritas, las normas especificadas o los términos de un contrato.*

Pasando a definiciones más precisas para el mundo de los negocios, la **Asociación Mundial de Cumplimiento** establece que:

> *...el* Corporate Compliance *es un conjunto de procedimientos y buenas prácticas adoptados por las organizaciones para identificar y clasificar los riesgos operativos y legales a los que se enfrentan y establecer mecanismos internos de prevención, gestión, control y reacción frente a los mismos.*

Para el **Comité de Basilea**, el cumplimiento es:

> *...una función independiente que identifica, asesora, alerta, monitorea y reporta los riesgos de cumplimiento en las organizaciones, es decir, el riesgo de recibir sanciones por incumplimientos legales o regulatorios, sufrir pérdidas financieras o pérdidas de reputación por fallas de cumplimiento con las leyes aplicables, las regulaciones, los códigos de conducta y los estándares de buenas prácticas.*

Para el portal **OroyFinanzas.com**, por cumplimiento se entiende la función específica que permite a las empresas, a través de procedimientos adecuados como el establecimiento de políticas de actuación en determinadas materias, detectar y gestionar los riesgos de incumplimiento de las obligaciones regulatorias, mitigar los riesgos de sanciones y las pérdidas que deriven de tales incumplimientos.

Coincido con Deloitte, cuando afirma que el *compliance* tiene una larga tradición en empresas de cultura anglosajona. Nace en los Estados Unidos de América (EUA) en los años setenta y ochenta, cuando tras grandes escándalos de corrupción y financieros que afectaron a importantes compañías, se dictó la ***Foreign Corrupt Practices Act*** o **FCPA** (1977), que incluyó requerimientos y prohibiciones en materia de sobornos, libros y registros.

La FCPA sirvió de modelo para más de 40 países de la Organización para la Cooperación y el Desarrollo Económico (OCDE) –incluyendo México– que han adoptado leyes similares. También resulta importante comentar que Reino Unido tiene su Ley contra el Soborno, de 2010 (*Bribery Act*). Los expertos afirman que estas dos son leyes extranjeras con impacto "extraterritorial".

¿CUÁLES SON LOS PILARES TRADICIONALES QUE CONFORMAN UN PROGRAMA DE *COMPLIANCE*?

Si estás en los EUA o trabajas para una empresa estadounidense, sin duda uno de los temas prioritarios que se atienden en un programa de *compliance* es el de antico-

rrupción. En México este tema también es primordial, desde la publicación de la Ley General del Sistema Nacional Anticorrupción (LGSNA) en 2016; la Ley General de Responsabilidades Administrativas (LGRA) de 2016 y las reformas –también de 2016– al Código Penal Federal (CPF) en materia de "delitos por hechos de corrupción", "ejercicio ilícito de servicio público" y "uso ilícito de atribuciones y facultades".

Otro de los temas que no pueden faltar en un programa de cumplimiento es el relacionado con la responsabilidad penal de las empresas. Con las reformas de 2016 al Código Nacional de Procedimientos Penales (CNPP) se formalizó la creación de un procedimiento sancionatorio para las personas morales.

De conformidad con lo establecido en el artículo 421 del CNPP, las empresas son "penalmente" responsables de los delitos cometidos a su nombre, por su cuenta, en su beneficio o a través de los medios que ellas proporcionen, cuando se haya determinado que además existió inobservancia del debido control en su organización.

El tercer pilar de casi todo programa de cumplimiento en las empresas es la prevención de operaciones con recursos de procedencia ilícita y financiamiento al terrorismo. Tal como lo comenta la firma EY, el *lavado* de dinero es un fenómeno internacional en el cual México se ubica como uno de los países con mayor incidencia de operaciones financiadas con recursos de procedencia ilícita. Por esta razón, nuestra nación, incorporándose a las exigencias globales, promulgó una ley que regula esas conductas ilícitas.

De esa manera, el objeto de la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (LFPIORPI), es proteger el sistema financiero y la economía nacional, estableciendo medidas y procedimientos para detectar actos u operaciones que involucren recursos de procedencia ilícita.

El cuarto eje de un programa típico de cumplimiento es en materia de competencia económica. Tal como lo sostiene la firma SAI Derecho y Economía, en México el creciente clamor por una efectiva aplicación de la legislación de competencia que combata prácticas comerciales que explotan ilegalmente el bolsillo de los consumidores y que desplazan a competidores, aunado al fortalecimiento y activismo de las autoridades de competencia, hace indispensable que las empresas –de todos los tamaños– se preocupen por conocer y asegurarse de respetar la normatividad de la materia.

Además de estos cuatro rubros que suelen estar contemplados en todo programa de cumplimiento, los que a veces se incluyen también son los que tienen que ver con el cumplimiento con regulaciones ambientales o financieras, en caso de ser aplicables para la empresa.

¿Por qué afirmo que el *compliance* es un dogma de fe? Porque todos los consultores, libros, artículos y en todas la conferencias y cursos sobre este tema, siempre te dicen lo mismo:

Tu programa de *compliance* debe incluir: anticorrupción; responsabilidad penal de las empresas; prevención de operaciones con recursos de procedencia ilícita, y competencia económica. Y de postre, todos terminan con la (misma) "cereza del pastel": cómo desarrollar el código de conducta y programa de integridad de la empresa.

¿CUÁLES SON LAS ÁREAS IGNORADAS USUALMENTE EN UN PROGRAMA DE *COMPLIANCE*?

Para un servidor, existen áreas que deben estar presentes en todo programa de cumplimiento de las empresas, y que siempre –o casi siempre– son ignoradas.

A diferencia de algunos de los pilares clásicos de los programas de cumplimiento, que no resultan siempre aplicables a todas las empresas, las áreas que mencionaré a continuación casi siempre están presentes en todas éstas, sin importar su giro.

Como la mayoría de las definiciones de *compliance* aluden a la función dentro de las empresas que tiene como objetivo primordial el detectar y gestionar los **riesgos de incumplimiento de las obligaciones regulatorias**, para poder explicar las áreas ignoradas, tengo que recurrir nuevamente a la definición de la **Asociación Mundial de Cumplimiento** que me parece más amplia:

> *Cumplimiento corporativo es un **conjunto de procedimientos** y **buenas prácticas** adoptados por las organizaciones para **identificar** y clasificar los **riesgos operativos y legales**.*
>
> *(Énfasis añadido.)*

Resulta prudente recordar que, para el **Comité de Basilea**, el cumplimiento no sólo se refiere a leyes aplicables sino también a **códigos de conducta** y a **estándares de buenas prácticas.**

Tomando en cuenta las previas "definiciones ampliadas" del concepto clásico de *compliance*, las áreas omitidas en los programas de esta materia son las siguientes:

1. Propiedad intelectual. Si bien no existe como tal un conjunto de "obligaciones" emanadas de la Ley de la Propiedad Industrial (LPI) o de la Ley Federal del Derecho de Autor (LFDA) que deban cumplimentar las empresas, lo cierto es que ser omisos en tomar ciertas precauciones en estas materias –que se traducen en buenas prácticas– puede generar riesgos operativos y legales para las organizaciones, los cuales las pueden llevar a tener pérdidas financieras o pérdidas de reputación.

2. Protección de datos personales. En esta materia es imposible negar la amplia carga regulatoria para todas las empresas. Cumplir con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) va mucho más allá de redactar y publicar un aviso de privacidad.

3. Seguridad de la información. En nuestro país existe una amplia variedad de leyes que establecen obligaciones específicas en materia de seguridad de la información, que usualmente se traducen en dotar a la información de tres atributos o principios: disponibilidad, integridad y confidencialidad. Otras normativas van más allá, y contienen obligaciones relacionadas con la prevención de fraudes y ataques cibernéticos, así como la obligación de contar con un soporte tecnológico seguro, confiable y preciso para sus clientes.

4. Entorno digital. La regulación de diversos aspectos del entorno digital en el cual nos desenvolvemos, como empresas y como personas, es cada vez más frecuente. Buena parte de la carga normativa en el ámbito digital tiene que ver precisamente con obligaciones en materia de protección de datos personales, protección de información confidencial y seguridad de la información.

Dado que las primeras tres *áreas ignoradas* en programas de cumplimiento tienen un fuerte componente o incidencia tecnológica, englobaré el enfoque principal de este artículo bajo el concepto de *compliance* digital.

¿QUÉ ES EL *COMPLIANCE* DIGITAL?

Para un servidor, el ***compliance* digital** es una función en las empresas que identifica, asesora, monitorea y reporta los riesgos derivados de incumplimientos a **leyes, reglas y estándares** en el ámbito digital y de los negocios electrónicos, que busca mitigar las consecuencias de esos riesgos, tales como: sanciones, pérdidas financieras, pérdidas reputacionales, entre otras, estableciendo mecanismos internos de prevención, gestión, control y reacción frente a los mismos.

Bajo este contexto, entendemos por:

1. Leyes: los códigos y normas (disposiciones legales del orden federal).

2. Reglas: los reglamentos y disposiciones secundarias o de carácter general.

3. Estándares: los códigos de ética, códigos de conducta, códigos de buenas prácticas, etcétera.

Los pilares del *compliance* tradicional, mientras no cambien las leyes respectivas, seguirán siendo los mismos durante años. Sin embargo, los detonadores que motivan el ***compliance* digital** no sólo derivan de leyes o regulaciones sino también de buenas prácticas que surgen ante la imperante necesidad de asegurar a la empresa en el siempre dinámico entorno tecnológico en el que vivimos.

Y, de hecho, por la misma naturaleza evolutiva del entorno digital, las leyes que lo regulan suelen cambiar con más frecuencia que el resto de la normatividad.

Puntos clave en un programa de *compliance* digital

1. Cumplimiento en materia de propiedad intelectual

Punto de control	Riesgos
Registro de marcas Licenciamiento de marcas	La empresa puede perder sus activos intangibles más valiosos si no se efectúa un adecuado control del portafolios de propiedad intelectual
Registro de programas de cómputo	La empresa podría no tener derechos sobre los programas informáticos que desarrolla internamente
Licenciamiento de programas de cómputo	Sin un adecuado control del *software* que se instala en las computadoras de los empleados, la empresa podría ser acreedora a sanciones considerables
Cláusulas de obra bajo relación laboral en los contratos individuales de trabajo	La empresa podría no ser titular de los derechos patrimoniales de los programas informáticos que desarrolla internamente
Contratos o cláusulas de obra por encargo con desarrolladores de *software* externos	La empresa podría no ser titular de los derechos patrimoniales de los programas informáticos que le desarrollan terceros

Uno de los problemas más recurrentes en las empresas –en el mejor de los casos– es el poder determinar contractualmente la correcta titularidad de programas de cómputo desarrollados tanto dentro como fuera de ésta. En el peor de los casos, tanto los contratos individuales de trabajo como los de desarrollo de *software*, son omisos en este tema.

Propiedad intelectual de creaciones hechas por trabajadores y profesionistas (*freelance*)

De acuerdo con el Dr. David Rangel Medina, en virtud de la clasificación de origen alemán, las invenciones hechas por los trabajadores se dividen en tres categorías:

a) Invenciones de servicio.

b) Invenciones de empresa.

c) Invenciones libres.

Invención de servicio es la que nace de investigaciones ordenadas por el patrón y efectuadas por el trabajador en el ejercicio de sus funciones respecto de las cuales es remunerado. También se les designa como "invenciones de empleados" en sentido estricto, debido a que son realizadas

cuando un contrato de trabajo o de prestación de servicio se celebra precisamente para producir la invención.

Invención de empresa es la que ha sido hecha por una persona que no está obligada por el contrato de trabajo a desarrollar una actividad inventiva, pero que para realizar el invento se basó primordialmente en conocimientos adquiridos dentro de la empresa en que trabaja y utilizó también medios proporcionados por ésta.

Invención libre es la que ha sido hecha por el trabajador por su propia iniciativa, fuera e independientemente del servicio para el que está obligado y sin el concurso de quien lo emplea.[1]

En el Derecho mexicano, las **invenciones de los trabajadores** están reguladas por dos ordenamientos: la LPI y la Ley Federal del Trabajo (LFT). Al respecto, la primera norma es bastante escueta, pues solamente admite la existencia de "invenciones laborales" y remite a la segunda norma.

Veamos a continuación lo que establece la LPI:

> ***Artículo 14.*** *A las invenciones, modelos de utilidad y diseños industriales realizados por personas que estén sujetas a una relación de trabajo, les será aplicable lo dispuesto en el artículo 163 de la Ley Federal del Trabajo.*

Nótese que este artículo contempla sólo tres figuras jurídicas reguladas por la LPI, que pueden estar presentes en una relación laboral:

- Las **invenciones**, las cuales son sujetas a protección vía patente. El término "invenciones" aparece recurrentemente en la LFT, según se verá más adelante.
- Los **modelos de utilidad.**
- Los **diseños industriales.**

Por su parte, los derechos del trabajador empleado y los de su patrón se rigen por el numeral 163 de la LFT, el cual a la letra señala lo siguiente:

> ***Artículo 163.*** *La atribución de los derechos al nombre y a la propiedad y explotación de las* ***invenciones*** *realizadas en la empresa, se regirá por las normas siguientes:*
>
> ***I.*** *El inventor tendrá derecho a que su nombre figure como autor de la* ***invención****;*
>
> ***II.*** *Cuando el trabajador se dedique a trabajos de investigación o de perfeccionamiento de los procedimientos utilizados en la empresa, por cuenta de ésta la propiedad de la* ***invención*** *y el derecho a la explotación de la patente corresponderán al patrón. El inventor, independientemente del salario que hubiese percibido, tendrá derecho a una compensación complementaria, que se fijará por convenio de las partes o por la Junta de Conciliación y Arbitraje cuando la importancia de la* ***invención*** *y los beneficios que puedan reportar al patrón no guarden proporción con el salario percibido por el inventor; y*
>
> ***III.*** *En cualquier otro caso, la propiedad de la* ***invención*** *corresponderá a la persona o personas que la realizaron, pero el patrón tendrá un derecho preferente, en igualdad de circunstancias, al uso exclusivo o a la adquisición de la* ***invención*** *y de las correspondientes* ***patentes.***
>
> *(Énfasis añadido.)*

Básicamente, en este artículo encontramos:

- El derecho moral del inventor asalariado (artículo 163, fracción I).
- El derecho del patrón al producto del trabajo (artículo 163, fracción II, primera parte).
- El derecho del trabajador a la remuneración de su trabajo (artículo 163, fracción II, última parte).
- Las invenciones libres del trabajador (artículo 163, fracción III).

Es importante resaltar que la norma laboral sólo habla de **"invenciones y patentes"**, pese a que la LPI establece que el artículo 163 de la LFT será aplicable también a **"modelos de utilidad"** y **"diseños industriales"** realizados por personas que estén sujetas a una relación de trabajo.

Hasta aquí hemos tratado el régimen jurídico de creaciones exclusivamente relacionadas con el mundo de la propiedad industrial, pero en el ámbito de los derechos de autor también existe regulación aplicable a obras realizadas por trabajadores.

En el Derecho anglosajón nace el concepto de ***work made for hire.*** Conforme al artículo 101 de la legislación de derechos de autor de los EUA (Título 17 del *U.S. Code*),[2] una "obra hecha por encargo" tiene el siguiente significado:

> *(1) una obra realizada por un empleado dentro del ámbito de su empleo; o (2) una obra especialmente ordenada o comisionada para su uso como una contribución a un trabajo colectivo, como una parte de una película cinematográfica u otra obra audiovisual, como una traducción, como obra complementaria, como compilación, como texto de instrucción, como una prueba, como material de respuestas para una prueba, o como un atlas, si las partes acuerdan expresamente en un documento escrito firmado por ellos que el trabajo será considerado una obra*

[1] Rangel Medina, David. "Los Derechos del Inventor Asalariado". *Revista Mexicana de la Propiedad Industrial y Artística.* Año VIII. 15-16. Enero-diciembre 1970. México, pp. 19-20

[2] *Copyright Law of the United States of America and Related Laws Contained in Title 17 of the United States Code.* Consulta realizada el 28 de julio de 2014. Véase en la página *web* de *Copyright* del Gobierno de los EUA: http://www.copyright.gov/title17/92chap1.html#101

hecha por contrato. A los efectos de la oración anterior, una "obra complementaria" es un trabajo preparado para su publicación como un complemento secundario a una obra de otro autor con el fin de introducir, concluir, que muestren, en la explicación, revisión, comentando, o ayudar en el uso de los otros trabajos, tales como prólogos, epílogos, ilustraciones pictóricas, mapas, gráficos, tablas, notas editoriales, arreglos musicales, material de respuestas para pruebas, bibliografías, apéndices e índices, y un "texto de instrucción" es una obra literaria, pictórica o la obra gráfica preparada para su publicación y con el propósito de su uso en la enseñanza escolar.

Por su parte, la LFDA regula de manera directa e indirecta el **"contrato de obra por encargo"** y el **"contrato de obra bajo relación laboral"** en los artículos 34, 83, 83 bis, 84 y 170, los cuales transcribo a continuación:

> ***Artículo 34. La producción de obra futura sólo podrá ser objeto de contrato cuando se trate de obra determinada cuyas características deben quedar establecidas en él.*** *Son nulas la transmisión global de obra futura, así como las estipulaciones por las que el autor se comprometa a no crear obra alguna.*
>
> *(Énfasis añadido.)*

> ***Artículo 83.*** *Salvo pacto en contrario,* ***la persona física o moral que comisione la producción de una obra*** *o que la produzca con la colaboración remunerada de otras, gozará de la titularidad de los derechos patrimoniales sobre la misma y le corresponderán las facultades relativas a la divulgación, integridad de la obra y de colección sobre este tipo de creaciones.*
>
> *(Énfasis añadido.)*

> ***Artículo 83 bis.*** *Adicionalmente a lo establecido en el Artículo anterior, la persona que participe en la realización de una obra musical en forma remunerada, tendrá el derecho al pago de regalías que se generen por la comunicación o transmisión pública de la obra, en términos de los Artículos 26 bis y 117 bis de esta Ley.*
>
> ***Para que una obra se considere realizada por encargo****, los términos del contrato deberán ser claros y precisos, en caso de duda, prevalecerá la interpretación más favorable al autor. El autor también está facultado para elaborar su contrato cuando se le solicite una obra por encargo.*
>
> *(Énfasis añadido.)*

> ***Artículo 84. Cuando se trate de una obra realizada como consecuencia de una relación laboral*** *establecida a través de un contrato individual de trabajo que conste por escrito, a falta de pacto en contrario, se presumirá que los derechos patrimoniales se dividen por partes iguales entre empleador y empleado.*
>
> *El empleador podrá divulgar la obra sin autorización del empleado, pero no al contrario.* ***A falta de contrato individual de trabajo por escrito, los derechos patrimoniales corresponderán al empleado.***
>
> *(Énfasis añadido.)*

> ***Artículo 170.*** *En las inscripciones*[3] *se expresará el nombre del autor y, en su caso, la fecha de su muerte, nacionalidad y domicilio, el título de la obra, la fecha de divulgación,* ***si es una obra por encargo*** *y el titular del derecho patrimonial.*
>
> ...
>
> *(Énfasis añadido.)*

Es importante resaltar lo señalado tanto en el artículo 163, fracción III de la LFT (en caso de invenciones libres del trabajador, la propiedad de la **invención** corresponderá a la persona o personas que la realizaron), así como en el numeral 84 de la LFDA (ante la ausencia de pacto contractual, se presumirá que los derechos patrimoniales se dividen por partes iguales entre empleador y empleado).

Como ha quedado asentado en párrafos precedentes, siempre será recomendable que la empresa o el patrón incluyan cláusulas especiales que regulen estos fenómenos de manera detallada, tanto en los contratos individuales de trabajo que celebren con sus trabajadores (obra bajo relación laboral) como en los contratos de desarrollo de *software* (obra por encargo).

2. Cumplimiento en materia de protección de datos personales

Pese a que la LFPDPPP ya cumplió nueve años de haber sido publicada, muchas empresas siguen pensando que tener el aviso de privacidad es más que suficiente. Tener su aviso de privacidad representa menos del 10% del cumplimiento de las obligaciones que marca la LFPDPPP.

De manera general, sin pretender ser exhaustivos, las principales obligaciones que hay que cumplir son las siguientes:

a) Los responsables en el tratamiento de datos personales deberán observar los principios de licitud, consen-

[3] Se refiere a las inscripciones de obra ante el Registro Público del Derecho de Autor

timiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la ley.

- Multas por incumplimiento: hasta $13'518,400 por cada concepto de violación.

b) Los responsables deberán permitir a los titulares, el ejercicio sin dilación de los derechos de acceso, rectificación, cancelación, oposición y revocación del consentimiento, previstos en la LFPDPPP.

- Multas por incumplimiento: hasta $27'036,800 por cada concepto de violación.

c) Todo responsable que efectúe el tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas, las cuales permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

- Multas por incumplimiento: hasta $27'036,800 por cada concepto de violación.

d) El responsable tendrá la obligación de dar a conocer a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad. Asimismo, el responsable deberá conocer cuáles son los tipos de avisos de privacidad que se establecen en la LFPDPPP y el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) (integral, simplificado y corto), sus respectivos contenidos, momentos y mecanismos de puesta a disposición.

- Multas por incumplimiento: hasta $13'518,400 por cada concepto de violación.

e) Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la presente ley. Asimismo, fomentará la protección de datos personales al interior de la organización.

- Multas por incumplimiento: Aunque no hay una multa específica por violación a esta obligación, la autoridad garante suele acomodar "áreas grises" como incumplimiento a alguno de los principios de protección de datos personales. En este caso, bien podría ser el principio de responsabilidad. Por tanto, la sanción podría ser de hasta $13'518,400 por cada concepto de violación.

f) El responsable deberá cumplir con todas las obligaciones relacionadas con la remisión y transferencia de datos personales, siendo particularmente relevante la formalización de las transferencias mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.

- Multas por incumplimiento: hasta $27'036,800 por cada concepto de violación.

De cada una de estas obligaciones derivan a su vez numerosos puntos de control. Sólo como ejemplo, para cumplir uno solo de los ocho principios en el tratamiento de datos personales, el de responsabilidad, el RLFPDPPP señala 10 medidas que podrán ser adoptadas.

Aunado a lo anterior, no basta con conocer la LFPDPPP y el RLFPDPPP, pues hay que saber también las particularidades involucradas en los requerimientos de la autoridad garante, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Cualquier reclamación, queja o denuncia relacionada con el ejercicio de los derechos Acceso, Rectificación, Cancelación y Oposición (ARCO), usualmente detona los siguientes requerimientos por parte del INAI:

- Precise la manera en cómo obtuvo los datos personales del denunciante.
- Acredite la forma en que el denunciante otorgó el consentimiento para que sus datos personales fueran utilizados por su representada y remita las documentales que acrediten su dicho.
- Acredite la forma en que su representada dio a conocer al denunciante su aviso de privacidad.
- Proporcione copia simple de su aviso de privacidad, indique la fecha de su elaboración y sus correspondientes modificaciones.
- Informe la manera en que su representada obtuvo el **consentimiento** (tácito) de la denunciante para el tratamiento de sus datos personales, así como el **consentimiento expreso** para **datos financieros y/o patrimoniales** e incluso el **consentimiento expreso y por escrito**, de haber obtenido datos personales sensibles.
- Aporte copia clara, completa y legible del documento a través del cual acredite que usted puso a disposición del denunciante su aviso de privacidad.
- Presente copia clara, completa y legible de su aviso de privacidad vigente al momento de los hechos denunciados y aplicable al denunciante.

La mayoría de las veces los responsables (las empresas) no son capaces de contestar con precisión los requerimientos del INAI, o no tienen los documentos de prueba necesarios para acreditar su dicho. El término para contestar al INAI sus requerimientos suele ser de cinco días hábiles. Si no trabajó a tiempo en su sistema de implementación de la LFPDPPP, lo más seguro es que no será capaz de producir los documentos (y las pruebas correspondientes) que le falten en ese corto periodo de tiempo.

3. Cumplimiento en materia de entorno digital

Cada empresa deberá atender las particularidades propias de cada uno de sus giros. En lo que respecta al entorno digital, lo mínimo que toda empresa debe cumplir son las obligaciones emanadas de la Ley Federal de Protección al Consumidor (LFPC) en materia de comercio electrónico.

En la celebración de transacciones efectuadas a través del uso de medios electrónicos se cumplirá con lo siguiente:

a) El proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción.

b) El proveedor utilizará alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informará a éste, previamente a la celebración de la transacción, de las características generales de dichos elementos.

c) El proveedor deberá proporcionar al consumidor, antes de celebrar la transacción, su domicilio físico, números telefónicos y demás medios a los que pueda acudir el propio consumidor para presentarle sus reclamaciones o solicitarle aclaraciones.

d) El proveedor evitará las prácticas comerciales engañosas respecto de las características de los productos.

e) El consumidor tendrá derecho a conocer toda la información sobre los términos, condiciones, costos, cargos adicionales, en su caso, formas de pago de los bienes y servicios ofrecidos por el proveedor.

f) El proveedor respetará la decisión del consumidor en cuanto a la cantidad y calidad de los productos que desea recibir, así como la de no recibir avisos comerciales, y

g) El proveedor deberá abstenerse de utilizar estrategias de venta o publicitarias que no proporcionen al consumidor información clara y suficiente sobre los servicios ofrecidos, en especial tratándose de prácticas de mercadotecnia dirigidas a la población vulnerable, como los niños, ancianos y enfermos, incorporando mecanismos que adviertan cuando la información no sea apta para esa población.

El incumplimiento a cualesquiera de las anteriores obligaciones podrá generar multas de la Procuraduría Federal del Consumidor (Profeco) de hasta $3'066,155.98 por cada concepto de violación.

Como se puede apreciar, estas obligaciones se dividen en:

a) Obligaciones de informar al consumidor (proporcionar domicilio, teléfono, costos, cargos, formas de pago, características de seguridad), las cuales se materializan con la publicación del documento ampliamente conocido como "términos y condiciones" en la página *web* de las empresas.

b) Obligaciones de tratar confidencialmente la información del consumidor y brindar seguridad a la misma.

c) Obligaciones de abstenerse de usar prácticas comerciales engañosas y estrategias publicitarias que no proporcionen al consumidor información suficiente y clara sobre los servicios ofrecidos.

d) Obligaciones de respetar la cantidad y calidad de los productos que el consumidor desea recibir.

En virtud de una reforma de noviembre de 2018 a la LFPC, ahora el proveedor que ofrezca, comercialice o venda bienes, productos o servicios utilizando medios electrónicos, ópticos o de cualquier otra tecnología, se guiará por las disposiciones de la norma mexicana expedida por la Secretaría de Economía (SE), la cual contendrá, por lo menos, la siguiente información:

a) Las especificaciones, características, condiciones y/o términos aplicables a los bienes, productos o servicios que se ofrecen.

b) Mecanismos para que el consumidor pueda verificar que la operación refleja su intención de adquisición de los bienes, productos o servicios ofrecidos y las demás condiciones.

c) Mecanismos para que el consumidor pueda aceptar la transacción.

d) Mecanismos de soporte de la prueba de la transacción.

e) Mecanismos técnicos de seguridad apropiados y confiables que garanticen la protección y confidencialidad de la información personal del consumidor y de la transacción misma.

f) Mecanismos para presentar peticiones, quejas o reclamos.

g) Mecanismos de identidad, de pago y de entrega.

Esta norma mexicana es la NMX-COE-001-SCFI-2018, la cual establece las disposiciones a las que se sujetarán todas aquellas personas físicas o morales que en forma habitual o profesional ofrezcan, comercialicen o vendan bienes, productos o servicios, mediante el uso de medios electrónicos, ópticos o de cualquier otra tecnología, con la finalidad de garantizar los derechos de los consumidores que realicen transacciones a través de esos medios, procurando un marco legal equitativo, que facilite la realización de transacciones comerciales, otorgando certeza y seguridad jurídica a las mismas. Se declaró la vigencia de esta norma en el DOF el 30 de abril de 2019.

Otro punto básico en un programa de *compliance* en el entorno digital se agrupa bajo la pregunta:

¿Quién está en control de tus activos digitales?

- **¿Qué podría suceder en su organización si el gerente o director de sistemas sale abruptamente de la empresa?** Usualmente, ante cualquier problema relacionado con computadoras, redes o información en la empresa, acudimos ante el director o área de sistemas, pero ¿quién vigila al vigilante? Si un problema se gesta al interior de este departamento, ¿cómo lo vamos a detectar y controlar? ¿Cómo mitigamos el riesgo de una salida abrupta de un directivo o funcionario clave del área de sistemas? No sólo es necesario tener un sólido respaldo contractual y esquema de políticas informáticas en la empresa, sino también destinar un apartado del *Business Continuity Plan* (BCP) para atender este riesgo.
- **¿Quién controla los nombres de dominio de su empresa?** Suele ser éste uno de los puntos más sensibles –y a la vez más ignorados– en las compañías. Perder su nombre de dominio no sólo implica "dejar de

existir" (aunque sea temporalmente) en Internet, sino que su empresa se quede sin correo electrónico, debido a que el mismo suele estar ligado a su nombre de dominio. Resulta indispensable revisar las bases de datos (*whois)* para verificar primeramente quién es el legítimo dueño (contacto registrante) de los nombres de dominio que presumiblemente pertenecen a la empresa. Es común que terceros e incluso el propio personal de sistemas registre a su nombre los dominios de la empresa. Ante una salida abrupta o imprevista del personal que tenga la administración y control (técnico y jurídico) de los nombres de dominio de la empresa, es necesario contar con el respaldo legal apropiado para poder recuperarlos a la brevedad posible.

"El error más grave que cometen los abogados de empresa es tratar los 'contratos de confidencialidad' como si fueran machotes o formatos sin importancia."

- **¿Quién controla las cuentas de redes sociales de su empresa?** De manera similar a los escenarios anteriores, es necesario reconocer la importancia que tienen las redes sociales en todas las empresas. Sin ellas, el contacto con el público, clientes potenciales, proveedores y otras partes interesadas (*stakeholders*) se reduce a su mínima expresión. Por comodidad, muchas veces las empresas contratan a *community managers* o a agencias de *marketing* digital para que les administren sus cuentas de redes sociales. Es muy común que se generen problemas con quien tiene a cargo esta importante labor. En los EUA cada vez son más comunes las "demandas por robo de *followers*" y demandas por daños y perjuicios en contra de *ex-community managers*, quienes por una mala administración o por actos dolosos o negligentes suelen meter en problemas a sus clientes. Un control contractual adecuado, aunado a revisiones periódicas, son necesarios para mitigar cualquier escenario adverso derivado de la tercerización de la administración de redes sociales.

Dependiendo de la industria de la cual su empresa sea parte, es posible que existan otras obligaciones específicas en cuanto al entorno digital se refiere. Tal es el caso de las instituciones de tecnología financiera, que deberán cumplir con un amplio catálogo de obligaciones digitales, especialmente en materia de seguridad de la información e infraestructura tecnológica, las cuales establece la Ley *Fintech*.

4. Cumplimiento en materia de seguridad de la información

La seguridad de la información es el conjunto de medidas preventivas y reactivas que adoptan las empresas, para permitirles resguardar y proteger su información buscando mantener tres atributos esenciales: la integridad, confidencialidad y disponibilidad de la información.

La **integridad** es el atributo que busca mantener los datos libres de modificaciones no autorizadas. Implica mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

La **confidencialidad** es el atributo que impide la divulgación de información a personas o sistemas no autorizados. Asegura el acceso a ésta únicamente a aquellas personas que cuenten con la debida autorización.

La **disponibilidad** de la información consiste en que ésta debe encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

El término "seguridad de la información" suele ser usado como sinónimo de "seguridad informática" o "ciberseguridad", lo cual es incorrecto.

La **seguridad de la información** busca proteger **activos basados en información**, almacenados o transmitidos sin el uso de Tecnologías de la Información y la Comunicación (TIC). La **seguridad informática** busca proteger **activos basados en información**, almacenados o transmitidos usando las TIC. La **ciberseguridad** busca proteger **activos no basados en información**, almacenados o transmitidos usando las TIC. Son "cosas informáticas" que no son información, pero son vulnerables a amenazas a través de las TIC.

Para efecto de este artículo, tomaré en cuenta controles de "seguridad de la información" y "seguridad informática".

Desde hace una década he venido pugnando por la creación del **derecho de la seguridad de la información**, que para mí es la rama de las ciencias jurídicas que busca un doble propósito:

a) Proteger a la información contenida en medios físicos, electrónicos y sistemas informáticos, contra daño, pérdida, alteración, destrucción, accesos y usos no autorizados, con la finalidad de conservar su confidencialidad, integridad y disponibilidad.

b) Brindar confidencialidad y seguridad a la información que sea: sensible, reservada, privada, secreto industrial, secreto bancario, secreto profesional, secreto técnico, secreto comercial, secreto de fabricación, dato personal, entre otros.

El error más grave que cometen los abogados de empresa es tratar los "contratos de confidencialidad" como si fueran

machotes o formatos sin importancia. En ellos, suelen tratar todo como secreto industrial, lo cual es incorrecto. Esta figura jurídica que protege información sensible de las empresas, está regulada por la LPI.

Para que se considere que existe un secreto industrial es necesario que concurran los siguientes requisitos (artículos 82, 83 y 223 de la LPI):

a) Que la información resguardada tenga aplicación industrial o comercial.

b) Que la persona resguarde la información con carácter confidencial.

c) Que la información le signifique obtener o mantener una ventaja competitiva o económica frente a terceros en la realización de actividades económicas.

d) Que el beneficiario de la información haya adoptado los medios o sistemas suficientes para preservar su confidencialidad y el acceso restringido a la misma.

e) La información de un secreto industrial necesariamente deberá estar referida a la naturaleza, características o finalidades de los productos; a los métodos o procesos de producción; o a los medios o formas de distribución o comercialización de productos o prestación de servicios.

f) La información deberá constar en documentos, medios electrónicos o magnéticos, discos ópticos, microfilmes, películas u otros instrumentos similares.

g) Para que sea delito su revelación indebida, debe habérsele prevenido al receptor de su confidencialidad.

México tiene una gran cantidad de leyes que protegen ciertos tipos de información sensible, como el secreto industrial, el secreto bancario/financiero, el secreto médico, el secreto profesional, el secreto técnico, los datos personales, entre otros.

Tradicionalmente, desde el punto de vista regulatorio, los contratos se dividen en "típicos" y "atípicos". Gracias a su ausencia regulatoria, los abogados hemos vivido décadas llamándole cómodamente al contrato más común de esta materia "contrato de confidencialidad" (incluso hay quienes le siguen llamando "convenio de confidencialidad").

Ante las necesidades del mundo digital en constante evolución en que vivimos, es necesario que migremos del "contrato de confidencialidad" al **"contrato de seguridad de la información".**

Ese contrato debe regular, cuando menos, temas de confidencialidad, seguridad de la información, seguridad informática y protección de datos personales.

COMENTARIO

Como se pudo apreciar, las necesidades en un programa de *compliance* van mucho más allá que las de sus clásicos pilares. Por ello, mantengamos una mente abierta y una actitud innovadora como abogados para poder proteger adecuadamente los activos digitales e intangibles de la empresa.