Ciudad de México, 9 de octubre de 2020

JUNTA DE COORDINACIÓN POLÍTICA
SENADO DE LA REPÚBLICA
LXIV LEGISLATURA
PRESENTE.

Asunto: Exposición del Proyecto de Trabajo

Estimada Junta:

En la actualidad las empresas no están exentas del valor agregado que pueden dar los datos personales que forman parte de sus activos, por lo que su debido tratamiento, se ha vuelto un tema relevante en los últimos años. Factores como el uso indebido de la información o la vulneración de medidas de seguridad de la misma, ponen en riesgo la reputación de las empresas, y las podrían hacer acreedoras de sanciones, por lo que resulta necesario estudiar el tema desde una perspectiva regulatoria, que incluya: legislación, normas sectoriales y buenas prácticas en materia de protección de datos y ciberseguridad.

En este sentido, las normas en el contexto nacional han contribuido a la construcción del derecho de protección de datos personales, y por ende a las obligaciones directas para el sector privado y empresas públicas, que, como parte de sus procesos, traten información.

El uso de las tecnologías de la información y comunicación están presentes en casi todos los procesos, lo cual ha optimizado sus recursos. Sin embargo, también han propiciado una serie de desafíos en torno a la seguridad de la información, la protección de los datos personales y el cumplimiento de la regulación en la materia.
En este sentido, para dimensionar la importancia que ha cobrado el derecho de la protección de datos personales, es necesario hablar del valor económico y social de la información al interior de las organizaciones. Esto debido a que la reputación y modelo de negocio de una empresa están basados en la confianza, estándares de protección de datos personales y medidas de seguridad de la información que se implementen.
En el mismo tenor, es importante conocer la dimensión de la regulación del derecho de protección de datos personales en posesión de las empresas de servicios establecidas en México, a través del razonamiento lógico normativo que permita analizar los principios y el cumplimiento de obligaciones y deberes en la materia, atendiendo a las características propias de este derecho humano.

Además tomando en consideración que nuestra vida diaria gira alrededor de actividades cada vez más digitalizadas y, por consiguiente, más sensibles a amenazas cibernéticas. Cadenas de suministro de alimentos, transporte, pagos y transacciones financieras, recolección y tratamiento de datos personales, trámites gubernamentales, servicios de emergencia, entre un sinnúmero de actividades, operan en la actualidad a través de tecnologías digitales. Las políticas de ciberseguridad son fundamentales para salvaguardar los derechos de los ciudadanos en el ámbito digital, tales como la privacidad, la protección de datos, así como para aumentar la confianza de los ciudadanos en las tecnologías digitales, y que éstos puedan sentirse cómodos accediendo a dichas tecnologías.

[redacted]

Identificar un peligro cibernético o vulneración de datos personales es tan sólo el primer paso. Tomar medidas contra las amenazas y crímenes del ciberespacio es un reto aún mayor para nuestro país. En la actualidad hay pocas capacidades para investigar los delitos que se cometen en el ciberespacio, incluso los relacionados con datos personales. Más aún, que dichos delitos resulten en juicio es todavía un reto mayor. Parte del problema se inicia muchas veces en la propia ley: en nuestro país no existe un marco legal sobre los delitos informáticos, ni se han suscrito a los convenios internacionales respectivos, cuando para un delito que no conoce fronteras, trabajar de la mano con otros países es un factor indispensable para el éxito.

Si bien nuestro gobierno es consciente de la necesidad de proteger el espacio digital y los datos personales del que tanto depende el funcionamiento de nuestra sociedad, la ciberseguridad no ha ganado presencia en la agenda política que se esperaría.

Las políticas y los marcos legales deben ajustarse y todas las partes interesadas de la sociedad civil, así como los sectores público y privado, deben trabajar para crear una cultura de protección de datos, privacidad y ciberconciencia y capacitar a profesionales calificados para construir una estrategia de ciberseguridad y una protección de datos más robusta; por lo tanto, es un esfuerzo continuo y complejo.

Contar con profesionales más capacitados se ha vuelto fundamental para diseñar e implementar las políticas y medidas de seguridad cibernética que son necesarias para garantizar la resiliencia del país frente a ciberataques cada vez más sofisticados y complejos, que muchas veces vulneran los datos personales en posesión del sector privado o público. México debe centrarse en mejorar el despliegue de estándares de seguridad de lo datos tanto física como cibernética y controles técnicos, así como fomentar el desarrollo de un mercado de ciberseguridad mas robusto y regulado que proteja a los cibernautas y sus datos personales.

En mayo de 2018 del Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) de la Unión Europea, el cual tiene un impacto significativo a nivel global. En la práctica, este ha sido un factor clave para que los líderes empresariales y las juntas corporativas comprendan mejor los riesgos cibernéticos de su modelo operativo comercial y logren el equilibrio adecuado entre proteger la seguridad de sus activos, mitigar las pérdidas y mantener la rentabilidad en un ambiente competitivo.

Esta mayor conciencia a nivel del liderazgo corporativo es un primer paso crucial para potenciar la toma de decisiones corporativas informadas para la planificación de la seguridad cibernética, los mecanismos de respuesta y las inversiones. Mientras tanto, a medida que las empresas más grandes han estado invirtiendo más en ciberseguridad y en innovación en materia de seguridad de datos, los análisis recientes señalan un aumento significativo de los ataques dirigidos a pequeñas y medianas empresas (pyme). Esto crea un riesgo significativo en el ecosistema digital, especialmente teniendo en cuenta que las pyme no tienen los recursos financieros para invertir fuertemente en ciberseguridad y la protección de sus datos, o simplemente la cultura de seguridad no constituye uno de los principales impulsores de sus agendas. Por lo tanto, aumentar la conciencia de seguridad cibernética y promover la higiene básica de seguridad cibernética y protección de datos en las pyme debe ser una prioridad [redacted] en los próximos años para el Gobierno.

Consecuentemente los objetivos primordiales de mi proyecto de trabajo son: bu[redacted] concientización sobre la importancia del derecho a la protección de datos persona[redacted] todos los sectores de la sociedad y su relación con la ciberseguridad; aportar la[redacted]

empresarial al Instituto sobre el valor económico y social de la información de clientes y usuarios en posesión de las empresas; determinar si el marco jurídico aplicable en dicha materia es suficiente y proponer la creación o cambios legislativos para la mejor protección de los mismos; conceptualizar el derecho a la protección de datos personales y ciberseguridad, así como especificar sus principios de interpretación; finalmente, analizar los desafíos que enfrenta el sector en el tratamiento de datos personales y ciberseguridad, así como sugerir mecanismos para el cumplimiento de la regulación en la materia y su mejoramiento.