

## **Foro Virtual Latinoamericano de Ciberseguridad**

29 de octubre, 2020

### **Reseña**

Los países latinoamericanos necesitan fortalecer sus capacidades en ciberseguridad, incorporar leyes que garanticen el uso responsable y seguro de la tecnología y responder a los desafíos de la digitalización de actividades cotidianas, afirmó la diputada María Marivel Solís Barrera (Morena), presidenta de la Comisión de Ciencia, Tecnología e Innovación.

Al inaugurar el Foro Virtual Latinoamericano de Ciberseguridad, Solís Barrera señaló que es fundamental crear capacidades a fin de que las instituciones públicas sean más eficaces para investigar y sancionar los delitos cibernéticos.

Dijo que las experiencias compartidas en esta jornada permitirán repensar cómo garantizar la seguridad de los usuarios de Internet y las redes globales. Ante ello, la adecuación de la legislación es vital para garantizar los derechos de los usuarios, ampliar el acceso y cerrar la brecha digital facilitando ambientes seguros y confiables, señaló.

La diputada Juanita Guerra Mena (Morena), presidenta de la Comisión de Seguridad Pública, afirmó que el reto es construir una legislación con énfasis en la protección a grupos vulnerables, que establezca la cooperación y aprovechamiento de casos de éxito en la materia. “Regular el Internet no es limitar las libertades, sino proteger a nuestras niñas, niños, adolescentes y mujeres”, estimó.

Refirió que las conductas delictivas cibernéticas son cada vez más graves y agresivas. Hay redes de pedofilia, tráfico de órganos o trata de personas que enganchan a las víctimas en redes sociales, o se lanzan retos que inducen al suicidio de jóvenes.

Se deben, agregó, adecuar las leyes, a fin de sancionar conductas virtuales de la misma manera en que se hace con las presenciales. Que el marco legal vaya al ritmo de la innovación y sea eficaz en el combate de los nuevos tipos delictivos.

La diputada María Eugenia Hernández Pérez (Morena) indicó que la ciberseguridad es estratégica para los países y las personas, pues los crímenes cometidos por este medio virtual son cada vez más sofisticados y representan un desafío para la sociedad.

Destacó la importancia de tipificar esos delitos, que en la pandemia se han multiplicado a través de clonación de teléfonos y cuentas bancarias, robo de identidad, fraudes, piratería, suplantación de personalidad y espionaje industrial. Además, afectan áreas estratégicas: comunicaciones, transportes e inteligencia civil y militar.

Añadió que éste es un avance en el esfuerzo de compartir conocimientos y experiencias legislativas en América Latina. “No llegamos tarde a este tema; estamos en tiempo para analizar y acompañar iniciativas que hagan una realidad la ciberseguridad”.

La senadora Beatriz Paredes Rangel, presidenta de la Comisión de Relaciones Exteriores para América Latina y el Caribe, afirmó que una de las cuestiones que más lastima en materia de ciberseguridad es la pornografía infantil. Se debe atacar con todo el rigor, recursos tecnológicos apropiados y la normatividad penal que corresponda.

El diputado Alfonso Pérez Arroyo (Morena) expresó que lo planteado en este foro ayudará a generar políticas públicas y el andamiaje legal más acertado en el tema de ciberseguridad.

## **Ciberseguridad en México**

El director de Ciberseguridad de la Secretaría de Seguridad y Protección Ciudadana, Javier Nieto Miranda, dijo que México está dentro de los 15 países más atacados en el mundo y el segundo lugar en América Latina. Se calcula que en 2019 el costo de los ciberataques fue de ocho mil millones de dólares. Quienes han sufrido más ataques son Pemex y las secretarías de Economía y la del Trabajo y Previsión Social, quienes tuvieron daños en su red informática interna.

Los ataques se presentan a través del Emotet, una red de robots informáticos o bots. De manera autónoma y automática se propagan a través de campañas temáticas, comienzan como un tipo de infección y terminan con un ransomware. Hoy está controlado, pero se espera que a finales de este año vuelva a tomar fuerza, afirmó.

## **Delitos financieros**

El consultor y especialista en ciberseguridad, Arturo García Hernández, consideró que para proteger la economía digital es importante forjar la cultura de prevención; además, la

adopción de la tecnología tiene que ser ágil y se necesita regular la moneda electrónica, Bitcoin. “Una tarea pendiente es atender el riesgo sistémico; estamos ante un efecto dominó que puede iniciar en alguna entidad financiera, con un usuario, que crece y no es atendido”.

### **La ley no tiene una definición clara sobre delitos cibernéticos**

El fundador de la organización Social TIC, Juan Manuel Casanueva, afirmó que la ley no tiene una definición clara de cuáles son los delitos cibernéticos. “El reto legislativo es la existencia de textos vagos y antiguos, no hay reglas enfocadas para atender delitos y acciones de ciberdelincuencia que pueden ser fácilmente identificados”. Destacó la importancia de diseñar una agenda intergubernamental porque no se puede decir que una ley resolverá todo.

### **Infraestructura y ciberseguridad**

El coordinador de Desarrollo Tecnológico de la Secretaría de Comunicaciones y Transportes, César Contreras González, subrayó que en la SCT implementó cinco ejes para el desarrollo tecnológico en diversos campos de las telecomunicaciones y la radiodifusión respecto de la transformación e inclusión digital. Se trabaja en identificar las nuevas tecnologías, monitorear tendencias tecnológicas, proponer recomendaciones y mejores prácticas, así como el uso seguro y responsable de las tecnologías de la información y comunicación (TIC).

### **Capital humano e investigación**

El coordinador de Proyectos en Ciberseguridad de ESIME Culhuacán, Gabriel Sánchez Pérez, mencionó que México tiene un déficit importante de generación de recursos humanos. “Es necesario que las universidades públicas y privadas que no consideran prioritario tener programas en ciberseguridad consideren que es tiempo idóneo para generar más recursos humanos en esto”.

### **Proceso incipiente, la regulación en ciberseguridad**

En el bloque dos se analizó la situación actual de la ciberseguridad a nivel regional, estadísticas, estrategias, tendencias, proyectos de ley vigentes regionales, su grado de avance y qué temáticas proponen. Participaron especialistas de México, Argentina, Costa

Rica y Paraguay.

Se indicó que hay un proceso incipiente y dispar en materia de regulación de ciberseguridad con un avance reactivo e iniciativas no integrales. Se consideró la importancia de mantener un enfoque de derechos humanos en la legislación específica; establecer estándares para que el sector privado tenga claras las reglas del manejo de datos personales.

### **Adaptar ley de protección de datos personales**

El vicepresidente del Comité de Ciberseguridad de la AIMX, Pablo Corona Fraga, propuso adaptar las leyes de protección de datos personales en posesión de particulares porque quedaron rebasadas, sobre todo en materia de consentimiento. Además, “tipificar y perseguir la pornografía infantil y el fraude, porque ha habido varias propuestas de ley que pareciera que buscan tipificar el uso de una herramienta en lugar de un comportamiento”.

### **Inteligencia artificial**

De CISO, HUAWEI en México, Martín Portillo habló sobre cómo impacta el uso de la inteligencia artificial en la ejecución de ciberdelitos y en los métodos de protección cibernéticos. Consideró necesario fijar límites a las plataformas en cuanto a la protección de datos.

### **Inversión en ciberseguridad**

De Intel México y director de Gobierno y Políticas Públicas, Íñigo Solana Riveroll, afirmó que se está ante la oportunidad de fortalecer el marco legal para tener un mejor sistema de ciberseguridad. Aseveró que el Gobierno requiere apropiarse del tema, verlo como prioridad e invertir. “Si no avanzamos en ciberseguridad, tampoco podremos hacerlo en temas de inteligencia artificial”.

### **Ciberseguridad debe ser prioridad del Gobierno**

El especialista Gilberto Villegas Montoya dijo que se debe abordar el tema de la ciberseguridad con buenas bases y que todos los sectores involucrados participen activamente en la elaboración de la legislación. Se pronunció por impulsar una cultura de ciberseguridad. “Debe ser un tema prioritario para la administración para desarrollar

políticas y no dejar morir el avance que se ha registrado en la materia”.

## Clausura

Finalmente, el diputado Brasil Alberto Acosta Peña (PRI) afirmó que es necesario legislar en temas de ciberseguridad a fin de tener un marco jurídico robusto. “En la Comisión somos plurales, porque el problema de ciberseguridad no le afecta a un individuo, independientemente el partido, le afecta a todos, por eso debemos trabajar unidos”.



**Comisión de Ciencia, Tecnología e Innovación**  
**Foro Latinoamericano de Ciberseguridad**

