



# Es urgente legislar en materia de ciberseguridad: Félix Castellanos

GRECIA ROSAS

En México el cibercrimen opera entre amplios vacíos legales y autoridades poco capacitadas; así, tan sólo en el primer trimestre de 2024, de acuerdo con reportes de la tecnológica Check Point, hubo en promedio 3 mil ataques semanales en el país, lo que representa un aumento interanual de 78 por ciento, denunció el especialista en Inteligencia para la seguridad nacional del Instituto Nacional de Administración Pública (INAP) Félix Castellanos Lucero.

Tras un análisis con expertos en el tema y diputados del Partido del Trabajo, con quienes elaboran una iniciativa de ley de ciberseguridad a nivel federal, Castellanos Lucero señaló que es urgente comenzar a legislar en la materia, ya que “no podemos quedarnos inmóviles ante una realidad que nos está superando desde hace 30 años”.

De acuerdo con el especialista, una de las problemáticas centrales es la ausencia de marcos normativos unificados, ya que existen contradicciones en la conceptualización de lo que es un delito en la red, a lo cual se suma la falta de definición de autoridades, que resulta en un panorama donde la respuesta y aplicación de sanciones es sumamente limitada y confusa.

Esto cobra relevancia ya que la red permite el funcionamiento de sectores de infraestructura crítica como energía, salud, bancos y comunicaciones alrededor del país, por lo que no sólo involucra pérdidas económicas que afectan a las empresas y al gobierno, sino que las vulneraciones a los sistemas mencionados también suponen un riesgo a la información de la ciudadanía en general.

Los actores de estos delitos operan como células organizadas que incluso llevan a cabo tareas de reclutamiento de menores por parte

del crimen organizado en plataformas de juegos como Roblox, “donde se identifican sectores vulnerables que estamos dejando en el abandono”.

Ante la complejidad de un escenario que evoluciona constantemente con nuevos métodos para cometer delitos por medio de Internet cada vez más destructivos, surgen cuestionamientos sobre las autoridades a cargo, ante lo cual el especialista destacó la necesidad de un fiscalía especializada e incluso un gabinete de seguridad cibernética que se guíe por los principios de un marco jurídico robusto, adaptado a los nuevos ilícitos.

“No se trata de llenar únicamente los vacíos, sino de comenzar a construir una cultura de ciberseguridad en la que nos cuestionemos qué hacer desde el momento del hackeo, para actuar de manera preventiva y no sólo desde la consecuencia, ya que es un tema que le debería interesar a todo el mundo.”