LA LEGISLATURA DE LA PROVINCIA DE SANTA FE SANCIONA CON FUERZA DE LEY

"FISCALÍAS ESPECIALIZADAS EN CIBERDELITOS Y EVIDENCIA DIGITAL"

ARTÍCULO 1° - Objeto –Créanse Fiscalías especializadas en Ciberdelitos y evidencia digital, las cuales tendrán a su cargo la investigación, colaboración y persecución de delitos siempre que para su comisión sean utilizados medios informáticos y sus derivados cometidos a través de la red.

ARTÍCULO 2° - Distribución Territorial. Las Fiscalías tienen las siguientes competencias territoriales y se establecerán de manera progresiva según decisión de autoridad de aplicación priorizando la siguiente distribución:

a)- 1 (una) Fiscalía Especializada en Ciberdelitos y Evidencia Digital para la Región Norte: comprende los distritos judiciales N°1 (Santa Fe); 19 (Esperanza); 5 (Rafaela); 18 (San Justo); 11 (San Jorge); 22 (Gálvez) N°20 (San Javier); 10 (San Cristóbal/Ceres); 15 (Tostado); 13 (Vera); 4 (Reconquista); y 17 (Villa Ocampo/Las Toscas); y,
b)- 1 (una) Fiscalía Especializada en Ciberdelitos y Evidencia Digital para la Región Sur: comprende los distritos judiciales N°2 (Rosario); 6 (Cañada de Gómez); 7 (Casilda); 8 (Melincué); 9 (Rufino); 12 (San Lorenzo); 14 Villa Constitución); y 16 (Firmat).

El asiento de cada Fiscalía será dispuesto por el Ministerio Público de la Acusación, a través del Fiscal General, pudiendo disponer que su sede sea rotativa o itinerante.

ARTICULO 3º: Funciones. Las Fiscalías especializadas en Ciberdelitos y

Evidencia Digital, intervienen en toda conducta delictiva que tenga por objeto sistemas o programas informáticos y/o que sea perpetrada a través de sistemas o programas informáticos. Estableciendo en su conformación y reglamentación las siguientes facultades y atribuciones:

A- Deberá investigar:

a)- Estafas y defraudaciones con utilización de medios informáticos y rasonware, phishsing, pharming, skimming;

b)- grooming;

c)- ataques de denegación de servicios;

d)- pornografía infantil por Internet u otros medios electrónicos;

e)- amenazas y coacciones cometidas por medios informáticos;

f)- extorsión o chantaje online bajo la modalidad denominada sextorsión;

g)- alteración, destrucción o inutilización de datos, documentos, programas o sistemas informáticos; y,

h) venta, distribución, circulación o introducción en un sistema informático de cualquier programa destinado a causar daños.

B- Deberá colaborar:

a)- En el apoyo técnico especializado a las demás unidades del Ministerio Público en el campo de la informática forense;

b)- en el cómputo estadístico de denuncias por ciberdelitos a nivel nacional junto con las demás Fiscalías;

c)- en la coordinación de los criterios de actuación y abordaje de la ciberdelincuencia junto con las demás Fiscalías y el Procurador General de la Provincia;

d)- en la coordinación, análisis y difusión de todos los datos relevados de las distintas fiscalías, que sirvan de herramienta como difusión de criterios de actuación en todo el territorio provincial para la información;

e)- en la colaboración y asistencia al MPA en cuestiones informáticas; y,

f)- en la determinación de puntos concientizadores y educativos sobre la implementación de medidas de seguridad informáticas, y el desarrollo y avance de las modalidades delictivas.

ARTÍCULO 4° - Competencia. Los conflictos de competencia que se susciten entre Fiscales y Fiscales Adjuntos, y Fiscales especializados en ciberdelitos y evidencia digital, serán resueltos por el Fiscal General del Ministerio Publico de la Acusación.

ARTÍCULO 5° - Autoridad de Aplicación. La autoridad de aplicación será el Ministerio Público de la Acusación mediante la reglamentación que dicte al respecto.

ARTÍCULO 6° - Composición. Cada Fiscalía estará compuesta por:

a) un (1) Fiscal en Ciberdelitos y Evidencia Digital y un (1) Fiscal Adjunto, conforme a las funciones y atribuciones previstas en la Ley N° 13.013 y modificatorias. Cada Fiscal será designado por Asamblea Legislativa a propuesta del Gobernador; y,
b) un equipo interdisciplinario que conformará el cuerpo de investigadores y brindará apoyo en el abordaje de las funciones enumeradas en el Artículo Nº 3.

ARTÍCULO 7° - Requisitos. Para desempeñar el cargo de fiscal se requerirá:

a) Título habilitante de abogacía con especialización según corresponda de por lo menos dos (4) años de antigüedad;
b) ciudadanía argentina; y,
c) dos (2) años de residencia inmediata en la Provincia, si no se ha nacido en ella.

ARTÍCULO 8° - Capacitación. Facúltase a la autoridad de aplicación a celebrar convenios de capacitación con Colegios Profesionales, Universidades y otras unidades especializadas en el territorio nacional.

ARTÍCULO 9°- Financiamiento. Autorizase al Poder Judicial a requerir las partidas presupuestarias para atender las erogaciones que demande el

cumplimiento de la presente ley.

ARTÍCULO 10° - Reglamentación. El Poder Ejecutivo de la Provincia de Santa Fe reglamentará la presente Ley dentro de los 120 (ciento veinte) días de su aprobación reasignando las partidas presupuestarias que se requieran para dotar de estructura humana y física adecuada a la función que le corresponde asumir.

ARTÍCULO 11° - Comuníquese al Poder Ejecutivo.

Sergio J Basile
Diputado Provincial

FUNDAMENTOS

Señor Presidente:

El avance y desarrollo de la tecnología ha implicado el surgimiento de nuevas formas de afectación a los bienes jurídicos de las personas utilizando medios informáticos para ello.

El desarrollo tan amplio de las tecnologías ofrece un aspecto negativo, el mismo ha abierto la puerta a conductas delictivas que se manifiestan de formas que hasta ahora no era posible imaginar. Este dinamismo plantea nuevos desafíos en materia de seguridad digital y corresponde dar tratamiento y respeto acorde con las nuevas circunstancias.

Se debe reconocer la influencia de la tecnología en este nuevo ordenamiento legal.

Es indudable que el uso de las tecnologías para la comisión de delitos ha convertido a cualquier ciudadano que envíe mensajes, utilice los servicios bancarios digitales o comparta sus fotos a través de internet, en objetivo de diversos tipos de ataques informáticos con el fin de afectar su honor, intimidad, propiedad, libertad, integridad sexuales, entre otros según el caso

La ciberdelincuencia se ha transformado en una de las mayores amenazas de la actualidad en la sociedad. El crecimiento de la conectividad a Internet viene ascendiendo a una velocidad sorprendente y de la mano de ello, los ciberdelitos.

Actualmente encontramos aquellos delitos que nunca podrían existir sin la informática y/o Internet. Entre ellos encontramos el grooming, phishing, spamming, infecciones informáticas por medio de virus o troyanos, programas maliciosos destinados a la denegación de servicio (DDoS), etc. También aparecen los delitos históricamente tipificados en los códigos penales para los que la tecnología incorpora una nueva forma de comisión a través de Internet. Podemos destacar, entre estos, las calumnias, extorsiones, estafas, hurto informático, violación de correspondencia, instigación a cometer delitos, y diferentes variantes de delitos sexuales como la pedofilia, pornografía.

Los ataques informáticos a escala mundial dirigidos a entidades públicas, privadas y personas aumentaron un 70 por ciento en la primera mitad de este año, signada por la pandemia de coronavirus, al pasar de 4.000 por semana en enero a 250.000 en mayo pasado, a través de 130 modalidades diferentes, según un estudio realizado por una consultora privada en ciberseguridad. El estudio destaca que, desde enero pasado, se

detectaron a nivel regional y global unos 907.000 mensajes vinculados al coronavirus usando las compras online como señuelo. Muchos grupos del crimen organizado han cambiado sus tácticas para explotar actualizaciones de pandemias y escasez de suministros, así como compras online, publicidad de productos esenciales, medicamentos falsos, beneficios fiscales y seguros de emergencia, usándolo como señuelo.

Respecto a los ataques informáticos vinculados con tarjetas de crédito, el estudio analiza que los registros maliciosos crecieron un 569%, incluyendo estafas, extracción de monedas no autorizadas, y dominios que tienen evidencia de asociación con sitios hechos por delincuentes. Los ataques se dieron a menudo a través de correos electrónicos donde los ciberdelincuentes se hicieron pasar por autoridades gubernamentales y de salud, incitando a las víctimas a que proporcionen sus datos personales y descarguen malware. El informe asegura además que los viejos esquemas de fraude, adecuados al contexto de la pandemia, han permitido a los ciberdelincuentes capitalizar las ansiedades y los temores durante la crisis, a tal punto que se produjeron 450 amenazas nuevas por minuto durante el primer semestre de 2020 en todo el mundo.

La organización Grooming Argentina estimó que desde el inicio del aislamiento, el delito de grooming aumentó el 30 % en el país ante la hiperconectividad de niñas, niños y adolescentes a internet y, según especialistas "uno de los mecanismos de captación viene de la mano del encierro, porque los chicos están aburridos y los padres les permiten jugar con el celular". El defensor del Pueblo Adjunto de Buenos Aires y responsable del Observatorio de Derechos de Niñas, Niños y Adolescentes, afirmó que "el grooming es uno de los delitos informáticos que más creció en los últimos años, incluso antes de la cuarentena, a punto tal que se abre una investigación penal cada 13 horas en la provincia". Desde la Unidad Especial de Violencia de Género, Familiar y Sexual de la provincia de Santa Fe, se alertó que "lo que está proliferando es un groomer que busca imágenes y

videos de desnudo o genital" pero no hay estadísticas actualizadas.

Estos delitos han tenido un aumento exponencial en los últimos tiempos. Y es por eso que requiere de profesionales especializados en constante capacitación, que puedan dar una respuesta tempestiva y efectiva con el conocimiento de las herramientas pertinentes.

Creemos que es deber del Estado y especialmente del Ministerio Público de la Acusación hacer frente de forma eficaz al problema, considerando la importancia del tema y tomando nuestra propuesta de creación de esta Fiscalía especializada en Ciberdelitos y Evidencia Digital.

Es necesario contar con instrumentos de cooperación y coordinación eficaces que permitan tanto a magistrados como funcionarios judiciales efectuar investigaciones expeditivas a fin de preservar los elementos de prueba referentes a las causas que instruyan. De ahí que se requiera también de disponer técnicas unificadas a nivel nacional para la prevención, investigación y persecución de aquellos.

En nuestro país, contamos con experiencias en este sentido, una de ellas es la Fiscalía de Instrucción especializada en Cibercrimen en la provincia de Córdoba. Se trata de la primera Fiscalía dedicada exclusivamente en la investigación de los delitos que se relacionan con la alta tecnología informática. Su creación data del mes de diciembre de 2018 cuando la Legislatura de Córdoba Sancionó la Ley N° 10593.

En la provincia de Chubut, la Procuración General del Ministerio Público Fiscal aprobó la Resolución N° 007/20 PG, que crea la Unidad Fiscal Especializada en Cibercrimen y Evidencia Digital (UFE CyED) con el objetivo de contar con magistrados, funcionarios y empleados idóneos para combatir los ciberdelitos. Se dota, así, al Ministerio Público Fiscal de una estructura dedicada a enfrentar los desafíos y dificultades que la complejidad

de los ciberdelitos demanda, poniendo énfasis en la capacitación de sus integrantes y la permanente actualización técnica y tecnológica en la materia de investigaciones en el ciberespacio.

Salta es otra de las provincias que recientemente creó una Fiscalía Penal especializada en Ciberdelincuencia y el cargo correspondiente, con competencia en todo el territorio salteño y con asiento en el Distrito Judicial del Centro.

En la Ciudad Autónoma de Buenos Aires, El Ministerio Público Fiscal cuenta con una Unidad Fiscal Especializada en Delitos y Contravenciones Informáticas (UFEDyCI), que se encarga de investigar todos los delitos y contravenciones cometidos a través de medios digitales.

En el Ministerio Público Fiscal de la Nación se encuentra la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI), cuyo fin es robustecer la capacidad de respuesta del organismo en materia de detección, persecución y represión de la criminalidad organizada y de los delitos que más menoscaban la seguridad ciudadana. Así la UFECI podrá entender en casos de ilícitos constituidos por ataques a sistemas informáticos, o cuando el medio comisivo principal o accesorio de una conducta delictiva incluya la utilización de sistemas informáticos, con especial atención en el ámbito de la criminalidad organizada, y crímenes en los que sea necesario realizar investigaciones en entornos digitales –aun cuando no hayan sido cometidos contra o mediante un sistema informático-.

Ante la necesidad de proteger a la sociedad frente a los ciberdelincuentes, que aprovechan las vulnerabilidades de los sistemas informáticos y el desconocimiento generalizado de la mayoría de las personas, presentamos este proyecto de ley, así como para también poder llegar a conformar un cómputo estadístico de la Provincia de Santa Fe en esta clase de delitos.

Por los motivos expuestos, solicito a mis pares acompañen el presente proyecto de ley.

Sergio J Basile
Diputado Provincial