



Proyecto de ley que modifica la ley N° 21.459, que establece normas sobre delitos informáticos, y la ley N° 18.168, General de Telecomunicaciones, para sancionar la suplantación de identidad mediante el envío de mensajes fraudulentos y establecer deberes de detección y bloqueo de dichas comunicaciones

I.- Antecedentes

En el último tiempo se ha extendido en nuestro país una modalidad de estafa conocida como *smishing*, consistente en el envío de mensajes de texto que aparentan provenir de bancos, empresas de autopistas concesionadas, servicios de encomienda u órganos públicos. El mensaje advierte al destinatario sobre una supuesta deuda del TAG, un problema con la entrega de un pedido o el bloqueo inminente de una cuenta, y lo insta a ingresar a un enlace que conduce a un sitio falso, diseñado para capturar claves, códigos de verificación y datos personales o financieros.¹

El fenómeno ha crecido de manera sostenida. La Policía de Investigaciones ha advertido que los intentos de este tipo de fraude aumentaron más de un treinta por ciento en el último año, y que sus principales víctimas son personas mayores o con menor familiaridad con los entornos digitales, precisamente aquellas a quienes la ley N° 21.459 quiso proteger de modo especial al contemplar una agravante por abuso de su vulnerabilidad.²

Frente a esta realidad, la respuesta institucional disponible es únicamente reactiva: la víctima puede denunciar ante el Ministerio Público, llamar al número de Denuncia Seguro o concurrir a Carabineros o a la Policía de Investigaciones una vez consumado el engaño. Nada

¹T13, “¿Problemas con el TAG o con la entrega de un pedido? Así puedes denunciar estafas por SMS fraudulentos”, 23 de julio de 2026. Disponible en: www.t13.cl.

²Según cifras de la Policía de Investigaciones de Chile, los intentos de smishing crecieron más de un treinta por ciento en el último año. Véase Diario Estrategia, “Smishing: la amenaza digital que llega al celular”. Disponible en: www.diarioestrategia.cl.

obliga hoy a impedir que el mensaje fraudulento llegue al teléfono de las personas, ni existe un tipo penal que capture con precisión la conducta de quien lo envía.

II.- Fundamentos

El ordenamiento vigente presenta dos vacíos que este proyecto busca corregir. El primero es de orden penal. El artículo 7° de la ley N° 21.459 sanciona el fraude informático, pero exige que se haya causado un perjuicio; el artículo 8° castiga el abuso de dispositivos, mas no comprende el envío del mensaje fraudulento en sí mismo.³ Por su parte, el artículo 214 del Código Penal, que castiga la usurpación de nombre, protege a las personas naturales y no alcanza la suplantación de empresas, marcas o servicios públicos, mientras que la ley N° 20.009 se circunscribe al uso fraudulento de tarjetas y transacciones electrónicas.⁴ El resultado práctico es que el envío masivo de mensajes que suplantán a una institución para capturar credenciales queda, en cuanto tal, sin sanción, salvo que logre acreditarse el fraude posterior y la participación del remitente en él, prueba que rara vez puede rendirse.

La forma más adecuada para subsanar el primer vacío, es la de los delitos de peligro, plenamente admitida en nuestro sistema cuando el adelantamiento de la barrera punitiva se justifica en la protección de bienes jurídicos relevantes. Aquí concurren varios: el patrimonio de las personas, la vida privada y la protección de los datos personales que asegura el artículo 19 N° 4 de la Constitución Política de la República, y la confianza en las comunicaciones electrónicas, soporte de una parte creciente de la vida económica del país.

El segundo vacío es de orden regulatorio. Los mensajes fraudulentos circulan por redes que operan concesionarios privados, quienes disponen de medios técnicos para detectar patrones de envío masivo, verificar remitentes y bloquear enlaces maliciosos, sin que la ley N° 18.168 les imponga deber alguno en tal sentido. La experiencia comparada avanza en la dirección contraria: España ha ordenado a los operadores bloquear llamadas y mensajes con identificadores falsificados⁵, y Costa Rica dispuso recientemente que las compañías móviles

³Artículos 7° y 8° de la ley N° 21.459, que establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest.

⁴Artículo 214 del Código Penal, en relación con el artículo 468 del mismo cuerpo legal; artículo 7° de la ley N° 20.009, que establece un régimen de limitación de responsabilidad para titulares o usuarios de tarjetas de pago y transacciones electrónicas en caso de extravío, hurto, robo o fraude.

⁵Orden TDF/149/2025, del Ministerio para la Transformación Digital y de la Función Pública del Reino de España, que impone a los operadores el bloqueo de llamadas y mensajes de texto con identificadores de origen falsificados.

implementen herramientas de detección y bloqueo de mensajes fraudulentos.⁶ Se trata de obligaciones dirigidas a empresas privadas, fiscalizables con las potestades sancionatorias que el artículo 36 de la misma ley, ya entrega a la autoridad, de modo que su incorporación no crea servicios públicos, no impone funciones nuevas a órganos del Estado ni irroga gasto fiscal.

III.- Idea Matriz

El proyecto persigue dos objetivos complementarios: sancionar penalmente, como delito de peligro, el envío de mensajes de texto u otras comunicaciones electrónicas que suplanten la identidad de órganos del Estado o de personas naturales o jurídicas con el propósito de capturar claves, credenciales o datos personales, y establecer el deber de los operadores de telecomunicaciones de detectar y bloquear dichas comunicaciones, resguardando así el patrimonio, la vida privada y los datos personales de las personas.

IV. PROYECTO DE LEY

Artículo 1º.- Incorpórese en la ley N° 21.459, que establece normas sobre delitos informáticos, el siguiente artículo 7º bis:

“Artículo 7º bis.- El que, con el propósito de obtener para sí o para un tercero claves de acceso, códigos de verificación, credenciales de seguridad, datos financieros o datos personales, enviare a una o más personas mensajes de texto u otras comunicaciones electrónicas atribuyéndose falsamente la identidad de un órgano del Estado o de una persona natural o jurídica, o que contuvieren enlaces u otros mecanismos de redirección a sitios, plataformas o aplicaciones que simulen ser de aquéllos, será sancionado con la pena de presidio menor en su grado mínimo a medio y multa de once a veinte unidades tributarias mensuales, aunque no se hubiere producido perjuicio.

⁶Resolución del Consejo de la Superintendencia de Telecomunicaciones de Costa Rica, de junio de 2026, que obliga a los operadores móviles a implementar herramientas de detección y bloqueo de mensajes fraudulentos. Véase Delfino.cr, “Operadores de telefonía móvil tendrán 18 meses para bloquear SMS fraudulentos”, junio de 2026.

Se impondrá el máximo de la pena señalada en el inciso anterior si los mensajes o comunicaciones se enviaren en forma masiva o mediante sistemas automatizados de distribución.

Lo dispuesto en este artículo se aplicará siempre que el hecho no constituyere un delito sancionado con una pena superior.”

Artículo 2º.- Agréguese en la ley N° 18.168, General de Telecomunicaciones, el siguiente artículo 24 L:

“Artículo 24 L.- Los concesionarios de servicio público de telecomunicaciones y quienes presten servicios de mensajería de texto o multimedia deberán adoptar medidas técnicas destinadas a detectar y bloquear el envío masivo de mensajes que suplanten la identidad de órganos del Estado o de personas naturales o jurídicas, o que contengan enlaces asociados a actividades fraudulentas.

Deberán, asimismo, verificar la identidad de quienes contraten servicios de envío masivo de mensajes con remitentes alfanuméricos y mantener un registro actualizado de dichos contratantes, el que deberá ser entregado al Ministerio Público o a los tribunales de justicia cuando lo requieran en conformidad a la ley.

Las condiciones técnicas de implementación de estas obligaciones serán las que determine el reglamento respectivo. Su incumplimiento será sancionado en conformidad al artículo 36.”

Artículo transitorio.- Las obligaciones establecidas en el artículo 24 L de la ley N° 18.168, incorporado por el artículo 2º de esta ley, comenzarán a regir transcurridos seis meses desde su publicación en el Diario Oficial.



ROBERTO ARROYO MUÑOZ
DIPUTADO DE LA REPÚBLICA