"Decenio de la Igualdad de Oportunidades para mujeres y hombres"
"Año de la recuperación y consolidación de la economía peruana"

LEY QUE MODIFICA EL DECRETO LEGISLATIVO N° 1182, PARA REGULAR LA GEOLOCALIZACIÓN DE TELÉFONOS MÓVILES QUE UTILIZAN NÚMEROS CON PREFIJO EXTRANJERO POR MOTIVOS DE SEGURIDAD

Los Congresistas de la República que integran el Grupo Parlamentario Bloque Democrático Popular, a la iniciativa del congresista **Edgard Reymundo Mercado**, al amparo de lo establecido en el Artículo 107° de la Constitución Política del Perú y de los artículos 75° y 76° del Reglamento del Congreso de la República, proponen el Proyecto de Ley:

Proyecto de Ley

EL CONGRESO DE LA REPÚBLICA
HA DADO LA SIGUIENTE LEY:

LEY QUE MODIFICA EL DECRETO LEGISLATIVO N° 1182, PARA REGULAR LA GEOLOCALIZACIÓN DE TELÉFONOS MÓVILES QUE UTILIZAN NÚMEROS CON PREFIJO EXTRANJERO POR MOTIVOS DE SEGURIDAD

Artículo 1.- Objeto de la ley
El objeto de la presente ley es mejorar la calidad de vida de la población, a través de mejorar la lucha contra la delincuencia, optimizando la labor de la Policía Nacional del Perú para hacer frente a la ciberdelincuencia.

Artículo 3. Modificación del Decreto Legislativo N° 1182
Modifíquese los artículos 2 y 3 del Decreto Legislativo N° 1182 Decreto Legislativo que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado, en los siguientes términos:

> *"Artículo 2.- Finalidad*
> *La finalidad del presente decreto legislativo es regular el acceso de la unidad especializada de la Policía Nacional del Perú, en casos de flagrancia delictiva o en investigaciones preliminares por el delito contra la vida, el cuerpo y la salud, el delito contra la libertad, el delito contra el patrimonio, delitos contra la administración pública, delitos de lavado de activos, delitos de trata de personas, delitos de tráfico ilícito de drogas, delitos de minería ilegal y los delitos comprendidos en la Ley 30077, Ley contra el Crimen Organizado, a la localización , geolocalización o rastreo de los teléfonos móviles y/o de cualquier otro dispositivo electrónico de comunicación,* ***incluyendo aquellos que a través de aplicativos, tarjetas SIM u procedimiento o tecnología, utilizan números con prefijo internacional estando en territorio nacional.***

Artículo 3.- Procedencia

La unidad a cargo de la investigación policial solicita a la unidad especializada el acceso inmediato a los datos de localización o geolocalización de teléfonos móviles o dispositivos electrónicos de naturaleza similar, ***considerados en el artículo 2 de la presente ley****, siempre que concurran los siguientes presupuestos:*

(…)

Artículo 4. Financiamiento
Lo establecido en la presente ley se ejecutará con cargo a los recursos institucionales del Ministerio del Interior y de la Policía Nacional del Perú. De manera complementaria se autoriza al Ministerio de Economía y Finanzas, de requerir, a identificar recursos presupuestales de manera complementaria.

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. – Ajustes normativos
El Poder Ejecutivo en un plazo no mayor de 90 días calendario realiza los ajustes normativos correspondientes para la ejecución de lo establecido en la presente ley.

SEGUNDA. – Campañas de sensibilización
El Ministerio del Interior, con cargo a su presupuesto institucional, impulsara campañas de información y sensibilización respecto a los riesgos relacionados a delitos como estafa, fraude, extorsión, chantaje, suplantación, entre otros, que se realicen a través de dispositivos móviles.

TERCERA. – Convenios y Asistencia Técnica
El Ministerio del Interior, en representación del Estado Peruano, queda autorizado a firmas convenios de cooperación o asistencia técnica con operadores de telecomunicación nacionales o extranjeros, con el fin efectuar una geolocalización o identificación efectiva de los dispositivos que utilicen números con prefijo internacional.

Lima, setiembre de 2025

FIRMA DIGITAL
Firmado digitalmente por: REYMUNDO MERCADO Edgard Cornelio FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 25/09/2025 11:54:18-0500

FIRMA DIGITAL
Firmado digitalmente por: ZEBALLOS MADARIAGA Carlos Javier FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 25/09/2025 13:15:07-0500

FIRMA DIGITAL
Firmado digitalmente por: REYMUNDO MERCADO Edgard Cornelio FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 25/09/2025 11:54:34-0500

FIRMA DIGITAL
Firmado digitalmente por: LUQUE IBARRA Ruth FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 25/09/2025 14:53:44-0500

FIRMA DIGITAL
Firmado digitalmente por: BAZAN NARRO Sigrid Tesoro FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 25/09/2025 12:12:27-0500

I. EXPOSICIÓN DE MOTIVOS

El aporte de las Tecnologías de la Información (TIC) es indudable. Desde hace varios años nuestra forma de estudiar, trabajar, interactuar o incluso distraernos ha cambiado. En nuestro caso, como país, este proceso de cambio se aceleró con la pandemia, pues descubrimos con más detalle el teletrabajo, la teleducación, el comercio electrónico, entre otros aspectos relevantes para nuestra vida diaria. Es claro que la implementación de TICs contribuye en diferentes aspectos de nuestra vida diaria. Lamentablemente estas tecnologías también son usadas para actos ilícitos.

Aprovechando el "*anonimato*" que ofrecen estas tecnologías, muchos delincuentes encuentran un escenario a favor para ocultar su identidad y tratar de engañar a sus interlocutores. Si bien cada dispositivo que se conecta a las redes cuenta con una dirección de protocolo IP o Dirección IP, los delincuentes están encontrando la forma de ocultarlos o de simular que se conectan de otros lugares.

Estos delincuentes no solo están al acecho para apropiarse del dinero de las cuentas o de las mercancías, también utilizando estas tecnologías para otros delitos que afectan a las personas como la trata de personas, la pornografía u otros.

Este cambio de nuestro modo vida es aprovechado por los delincuentes para identificar vulnerabilidades y sacar provecho a su favor. Hoy en día, ya no solo somo acechados en las calles, medios de transporte o en nuestro hogar, también lo podemos estar a distancia por personas, que aprovechando de esta estructura que se ha concebido, traspasan fronteras y nos atacan. Al respecto la INTERPOL señala[1]:

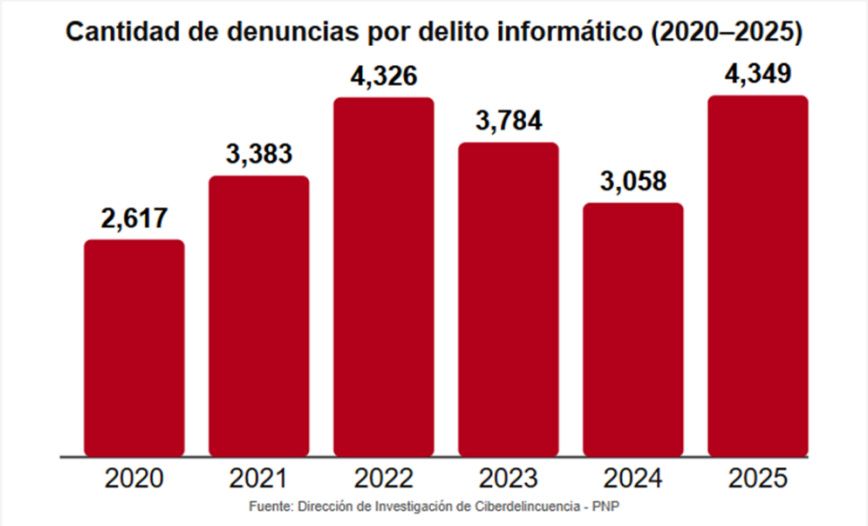
> **La ciberdelincuencia traspasa fronteras y evoluciona a gran velocidad**
>
> Hoy en día, el mundo está más conectado digitalmente que nunca. Los delincuentes se están aprovechando de esta transformación en línea para atacar, a través de sus puntos débiles, las redes, infraestructuras y sistemas informáticos. Esto tiene una enorme repercusión económica y social en todo el mundo, tanto para los gobiernos, como para las empresas o los particulares.

[1] https://www.interpol.int/es/Delitos/Ciberdelincuencia

El phishing, el ransomware y las violaciones de la seguridad de los datos son solo algunos ejemplos de las actuales ciberamenazas, eso sin contar que continuamente están surgiendo nuevos tipos de ciberdelitos. Los ciberdelincuentes son cada vez más ágiles y están mejor organizados, como demuestra la velocidad con que explotan las nuevas tecnologías, y el modo en que adaptan sus ataques y cooperan entre sí de forma novedosa.

Los ciberdelitos no conocen fronteras. Los delincuentes, las víctimas y las infraestructuras técnicas están dispersos por múltiples jurisdicciones, lo que resulta muy problemático a la hora de realizar una investigación o emprender acciones judiciales.

Nuestro país no ha sido ajeno a esta situación. Según datos de la División de Investigación de Ciberdelincuencia de la Policía Nacional del Perú, las denuncias por delito informático pasaron de 2,617 en el 2020 a 4,349 en el 2025 (hasta el mes de julio)[2]. Se proyecta que la información al 2025 sea el doble de lo registrado en el 2024.



La suplantación de identidad o el fraude informático son las principales moda lides que utilizan estos delincuentes, de acuerdo con la información de la Policía Nacional del Perú.

Las modalidades más comunes son[3]:

[2] https://andina.pe/agencia/noticia-estas-son-las-modalidades-delitos-informaticos-mas-denunciadas-el-peru-969892.aspx
[3] https://andina.pe/agencia/noticia-estas-son-las-modalidades-delitos-informaticos-mas-denunciadas-el-peru-969892.aspx

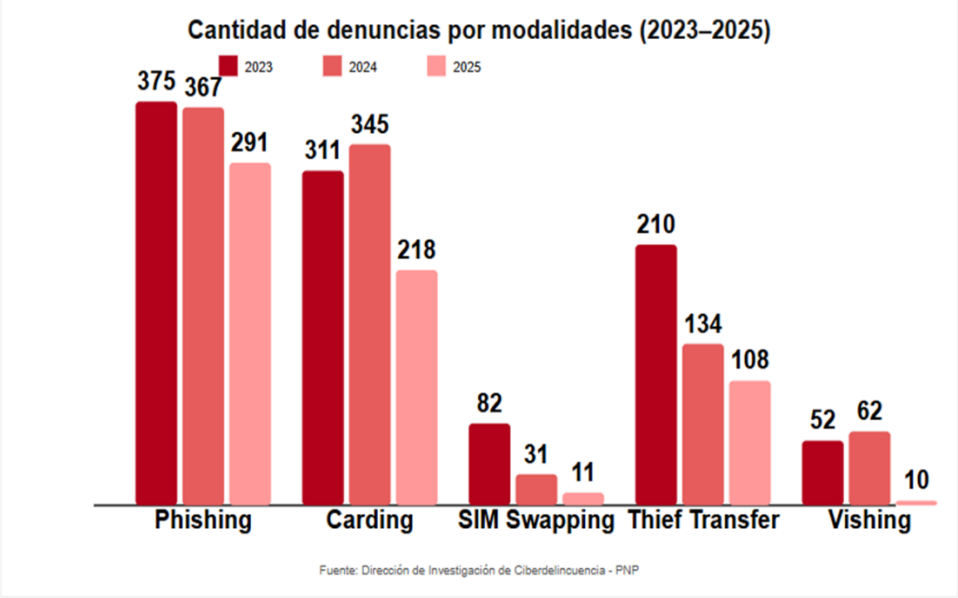
Phishing. Que consiste en la clonación de una pagina web, regularmente de entidades financieras, a fin de obtener datos como nombre, DNI e incluso las claves de sus cuentas.

Carding. Compra en línea luego de acceder a la información de las cuentas o tarjetas de terceros. En ocasiones se suplanta la identidad del titular.

Thief Transfer. Es el uso de celulares extraviados o robados obtener información y realizar por ejemplo transferencias de las cuentas de los titulares de los equipos. En ocasiones también se poner comunicación con los contactos que encuentren en los equipos para solicitar dinero a través de transferencias.

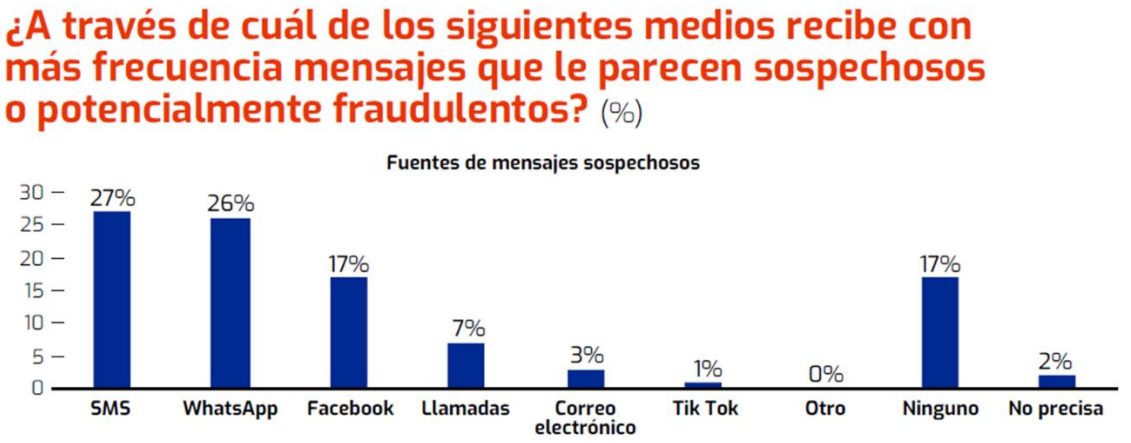
SIM Swapping. Los delincuentes con la información y los equipos de terceros, gestionan nuevas líneas ante las empresas de telecomunicaciones, para luego acceder a plataformas financieras y solicitar préstamos, sustraer dinero o hacer transferencias.

Fake APP. Esta modalidad esta en crecimiento debido al mayor uso de billeteras electrónicas o aplicativos como Yape o Plin, así como tiendas virtuales como Temu, Shein o Aliexpress.



Los medios por donde "ataca" la ciberdelincuencia ha dejado de ser predominantemente las llamadas telefónicas. Hoy día son los canales digitales los medios por donde se han identificado estos ataques como SMS, Facebook o Whatsapp. Los mensajes de texto o SMS son administrados por las empresas operadoras y regulados por OSIPTEL, no están anclados a una conexión a internet y operan a través de la red móvil del teléfono celular. La figura es diferente para las redes sociales como Facebook, Whatsapp, Instagram o TikTok,

que operan a través de internet y no se encuentran reguladas por OSIPTEL, por lo que el contenido no puede necesariamente ser regulado por autoridades nacionales. *Además, carecemos de una legislación específica que obligue a una coordinación rápida entre Meta y los operadores de justicia en casos de delitos como extorsión o estafa*[4].



Estas nuevas modalidades de crimen buscan ser erradicadas de nuestra sociedad. Para tal fin se dio Decreto Legislativo Nº 1182 - Decreto Legislativo que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado, que como lo describe su articulo 1 busca hacer frente a la codelincuencia:

Artículo 1.- Objeto

El presente decreto legislativo tiene por objeto fortalecer las acciones de prevención, investigación y combate de la delincuencia común y el crimen organizado, a través del uso de tecnologías de la información y comunicaciones por parte de la Policía Nacional del Perú.

Este es un avance importante, sin embargo, la aplicación de dicho decreto legislativo se ve limitado, toda vez que los delincuentes trascienden fronteras con su accionar, y la policía nacional tiene que operar dentro de la jurisdicción nacional.

Un tema que no debemos dejar de lado es la rápida evolución de esta "actividad", que no solo se ha hecho fuerte en el campo de la "tecnología de la información", sino que además esta migrando hacia el campo de la "tecnología de la operación". Hoy en día, los bancos y entidades financieras han redoblado

[4] Observatorio del Crimen y la Violencia. BCP. Junio 2025. Disponible en: https://bancodeideascredicorp.com/media/Reporte_BCP_2025-junio.pdf

esfuerzos para mejorar su seguridad, y se vuelven menos vulnerables. Por esa razón los ciberdelincuentes han puesto la puntería ahora en aeropuertos, hospitales, plantas de energía o manufacturas, ampliando las posibilidades de hacer daño a la arquitectura de la economía[5].

Es por lo anterior, que se requieren tomar medidas inmediatas a fin de que cortar esta tendencia creciente del uso de las tecnologías de información, aprovechando el anonimato y además la facilidad que tienen estos delincuentes aparentar no estar en el país.

II. ANALISIS COSTO BENEFICIO

La presente iniciativa no plantea una demanda directa de recursos presupuestales, toda vez que las autoridades nacionales ya cuentan con una estructura para llevar a cabo geolocalización, tal como se establece en el Decreto Legislativo N° 1182. Lo que se busca es darle marco para que puedan geolocalizar aquellos equipos que aprovechan la tecnología para aparentar que o están en el territorio nacional. Se estima que se requerirán ajustes a la estructura con que cuenta actualmente la Policía Nacional del Perú o capacitación y asistencia técnica para los ajustes correspondientes.

Por otro lado, respecto a los beneficios, ampliar las posibilidades de acción de las autoridades nacionales para hacer frente a la ciberdelincuencia, contribuirá a actuar de manera oportuna y por ende a reducir los índices de criminalidad en nuestro país, mejorando la calidad de vida de los ciudadanos. Como dato, en el 2024, los ciberdelincuentes robaron un total de S/ 90 millones solo en Lima Metropolitana, y a nivel nacional se reportaron 42 mil denuncias por delitos informáticos[6].

III. EFECTOS DE LA VIGENCIA DE LA NORMA EN LA LEGISLACION NACIONAL

La presente iniciativa legislativa no colisiona con ninguna norma de rango constitucional ni con las normas de nuestro ordenamiento nacional. Por el contrario, busca hacer precisiones al marco legal vigente, enmarcado en el Decreto Legislativo N° 1182 Decreto Legislativo que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado.

[5] https://www.ey.com/es_pe/insights/cybersecurity/ciberseguridad-riesgos-pasaron-frontera-ti
[6] https://rpp.pe/peru/actualidad/fraudes-digitales-y-suplantacion-de-identidad-alarmantes-cifras-de-la-pnp-revelan-el-impacto-de-la-ciberdelincuencia-en-peru-noticia-1620466

IV. VINCULACION CON EL ACUERDO NACIONAL Y SUS POLITICAS NACIONALES

La presente iniciativa se enmarca en las siguientes políticas del Acuerdo Nacional:

Política 7: Erradicación de la violencia y fortalecimiento del civismo y de la seguridad ciudadana

(f) desarrollará una política de especialización en los organismos públicos responsables de garantizar la seguridad ciudadana

Política 9: Política de Seguridad Nacional

(a) fomentará la participación activa de toda la sociedad en su conjunto, en el logro de objetivos de la política de seguridad nacional