SESIÓN N° 7, DE SUBCOMISION DE CRIMEN ORGANIZADO PERÍODO LEGISLATIVO 2022-2026, CELEBRADA EL MARTES 03 DE JUNIO DE 2025. SE ABRE A LAS 17.35 HORAS.

SUMARIO.

La Subcomisión se reunió con el propósito de tratar "el robo de aparatos de telefonía móvil como delito conexo del crimen organizado".

I.- PRESIDENCIA

Presidió la sesión, el diputado Diego Schalper Sepúlveda p**residente** titular, actuó como abogado secretario la Comisión, el señor **Mario Rebolledo Coddou**, como Abogado Ayudante, el señor **Hugo Balladares Gajardo** y como secretaria, la señora **Claudia Mora.**

II. ASISTENCIA.

Asistieron los integrantes de la subcomisión los diputados Andrés Longton, Raúl Leiva y Diego Schalper Sepúlveda.

Concurrieron como invitados el subsecretario de Telecomunicaciones, señor Claudio Araya San Martín: la Subdirectora de la Unidad Especializada en Crimen Organizado y Drogas del Ministerio Público, señora Tania Gajardo Orellana; el Prefecto jefe Nacional Contra Robos y Focos Criminales de la Policía de Investigaciones, señor Marco Ramírez Álvarez; y el presidente Ejecutivo de Chile Telcos, señor Alfie Ulloa Urrutia.

III. CUENTA.

1. Correo electrónico del Gabinete del fiscal nacional, excusando su participación a la sesión de hoy, sin embargo, en representación del Ministerio Público y en forma telemática, participará la subdirectora de la Unidad Especializada en Crimen Organizado y Drogas, Señora Tania Gajardo Orellana.

2. Excusas del director general de la Policía de Investigaciones, quien por actividades propias del cargo agendadas con anterioridad, no podrá asistir a la sesión de hoy, sin embargo, en su representación asistirá el prefecto Marco Ramirez Álvarez, jefe nacional contra robos y focos criminales.

IV. ACUERDOS.

Oficiar a la Policía de Investigaciones de Chile y al Ministerio Público, respecto a la cantidad de casos de robos por sorpresas de aparatos telefónicos.

V. ORDEN DEL DÍA.

La Subcomisión se reunió con el propósito de tratar "el robo de aparatos de telefonía móvil como delito conexo del crimen organizado". Para tales efectos expusieron:

El señor **Claudio Araya San Martín**, subsecretario de Telecomunicaciones, indicó que le parecía muy pertinente la invitación, aunque no se manejaba mucho en el tema de seguridad. No obstante, señaló que desde hacía aproximadamente dos años y medio se venía impulsando una agenda de seguridad desde el mundo de la tecnología digital, lo cual surgió a raíz de contrataciones como las que se planteaban en la instancia.

Explicó que, como consecuencia de ello, hacia fines del año 2022 se implementó una norma que obligaba a las empresas de telecomunicaciones a bloquear los teléfonos robados antes de su comercialización. Detalló que, antes de esa normativa, si a una persona le robaban un teléfono, este se bloqueaba en una base de datos a la que accedían las redes de telecomunicaciones para cursar llamadas y entregar servicio, inhabilitando el aparato para cursar tráfico. No obstante, los teléfonos que no tuvieran asignada una línea —como aquellos robados en tránsito desde la importación hasta la venta— no eran bloqueados. A partir de la norma de 2022, esos equipos también quedaban sujetos a bloqueo.

Señaló que esto permitió visualizar una disminución en la cantidad de reclamos por asaltos a bodegas, aunque reconoció que estos seguían ocurriendo. Aclaró que el sistema de bloqueo era imperfecto, ya que existían servicios técnicos que podían adulterar el IMEI (número único que identifica un teléfono). Indicó que, si el bloqueo dependía exclusivamente del IMEI, podía volverse inefectivo en poco tiempo.

En este contexto, informó que se encontraba en elaboración una nueva norma técnica, con fecha de compromiso al 31 de julio, que buscaba bloquear al menos dos factores —idealmente tres— para hacer más efectivo el sistema. Esos factores eran: el IMEI, el número de línea (por ejemplo, el +569) y la identidad internacional del abonado, que identificaba la red a la que el teléfono estaba asignado. A su juicio, el bloqueo simultáneo del IMEI y alguno de estos dos atributos permitiría una mayor eficacia, aunque reconoció que seguirían existiendo tareas pendientes.

Entre otras medidas implementadas, mencionó que en febrero se generó revuelo debido a la puesta en marcha de la verificación biométrica de identidad. Gracias a esto, todos los contratos de telecomunicaciones requerían la participación de un adulto responsable mayor de 18 años, incluyendo los servicios prepago. Además, recordó que el Congreso aprobó una ley que obligaba al registro de los prepagos. Aunque este registro aún no se implementaba, explicó que se estaba elaborando la norma técnica correspondiente. Una vez en marcha, no habría dispositivos generando tráfico a través de redes públicas sin un usuario responsable asociado, salvo en el caso de teléfonos robados. Sin embargo, al avanzar hacia un bloqueo más efectivo, se esperaba facilitar a los persecutores la identificación de responsables de tráfico malicioso.

Añadió que, en materia de portabilidad numérica, se implementó una verificación adicional para usuarios de pospago, lo cual antes no existía. Esto, según dijo, permitía que se produjeran portabilidades no solicitadas, las que representaban una defraudación al usuario y también una herramienta para delinquir mediante la obtención ilegítima de líneas telefónicas.

Indicó que quedaban pendientes dos aspectos: determinar qué hacer con los IMEI ya adulterados, dado que existía una gran cantidad de dispositivos sustraídos que habían sido comercializados en el mercado negro y activados lícitamente por usuarios, y abordar los casos en que varios dispositivos compartían un mismo número IMEI, lo que dificultaba saber cuál era el legítimo. Sostuvo que se venía trabajando en este aspecto con empresas como Chile Telco, debido a su información más actualizada, y remarcó que se trataba de una situación dinámica, sujeta al recambio de equipos y a la persistencia del robo de teléfonos.

Precisó que se estaban buscando mejores formas de bloqueo para que un teléfono

robado se convirtiera en algo tan inútil como un pisapapeles. No obstante, advirtió que se trataba de una tarea difícil. Señaló que la Policía de Investigaciones (PDI) podría fundamentar mejor lo complejo que era evitar la salida de teléfonos robados del país, ya que eran muy fáciles de reducir y transportar.

Por esa razón, se incorporó una regulación que exigía que, cuando se robara un teléfono en Chile, este fuera inscrito en una lista mantenida por la GSMA, una asociación de organizaciones dedicadas a la telefonía móvil a nivel global. Esta base de datos global de dispositivos robados permitiría evitar que teléfonos robados en el extranjero ingresaran a Chile y fueran comercializados ilegalmente.

Recalcó que no se trataba de una tarea sencilla y que era necesario un esfuerzo considerable para que estas medidas fueran efectivas. Finalmente, indicó que todo este conjunto de normativas había buscado reducir la utilidad de los teléfonos robados y garantizar la trazabilidad de las líneas telefónicas utilizadas en delitos, para poder identificar a los responsables. Mencionó además una actualización al decreto de interceptación y la normativa del Código Procesal Penal que obligaba a las compañías a entregar información a los persecutores cuando se investigaban líneas telefónicas por desaparición de personas o sospechas fundadas de vinculación con organizaciones criminales.

En resumen, afirmó que se trataba de un conjunto de medidas —algunas administrativas, vía resoluciones o decretos, y otras legislativas— orientadas a generar un marco normativo que permitiera la detección temprana y la persecución adecuada de actividades delictuales relacionadas con el uso de dispositivos móviles.

******

El señor **Alfie Ulloa Urrutia** presidente Ejecutivo de Chile Telcos, señaló que este era un tema en el que venían trabajando desde hace tiempo con la Subsecretaría y con el Congreso. Indicó que existía una agenda amplia en materia de seguridad de redes, equipos, baterías, cables de cobre, así como seguridad de los clientes y en redes digitales, incluyendo aspectos de autentificación.

Precisó que, con la ley de registro prepago, estaban obligados a almacenar información de cada cliente durante cinco años, lo que implicaba el manejo de diversos datos personales. Aclaró que lo que se empadronaba no eran los aparatos, sino los números telefónicos, aunque ello también implicaba registrar características del equipo y del usuario. Explicó que la autenticación biométrica era el mecanismo previsto para empadronar, junto con la información proporcionada por el usuario, aunque reconoció que no eran notarios para verificar domicilios.

Indicó que, además de los datos del individuo, se incluían características del equipo (el o los IMEI) y del número telefónico, el cual podía mantenerse incluso al cambiar de compañía, lo que hacía necesario considerar también el identificador de la tarjeta SIM. Esta combinación de identificadores —del equipo, del número y del usuario— fue denominada como “la tríada”.

Señaló que esperaban una norma técnica que entregara mayor detalle al respecto y que ya contaban con experiencia en autenticación biométrica, exigida hoy para trámites a distancia o en sucursal, lo que permitía asegurar, al menos, que la persona que adquiría una tarjeta estuviera debidamente identificada, aunque no se podía garantizar que esa persona fuera quien finalmente usara el aparato.

Comentó que, debido a las características del mercado chileno, era más atractivo ser cliente de postpago que de prepago, ya que los planes eran ilimitados, algo que no ocurría en otros países de América Latina. Esta situación explicaba la reducción de clientes de prepago, que ahora ascendían a unos siete millones, y que eran los que debían ser empadronados.

Agregó que contaban con una base de datos centralizada donde se registraban todos los teléfonos que operaban en Chile, una base temporal para turistas o

personas que traían equipos del extranjero, y una base histórica más extensa. Precisó que había aproximadamente cinco millones y medio de IMEI duplicados en la base actual, pero que el número de equipos en uso alcanzaba los 25 millones. Mencionó que los 127 millones de equipos históricos incluían muchos dispositivos del Internet de las Cosas, como sensores.

Explicó que los duplicados podían deberse a modificaciones realizadas en talleres, donde se cambiaba digitalmente el IMEI, ya fuera copiando un IMEI legítimo o generando uno nuevo. Esta práctica permitía que teléfonos robados siguieran operando en el mercado de segunda mano. Relató un ejemplo personal para ilustrar el problema: al reparar un teléfono, su IMEI legítimo podía ser copiado y reutilizado en miles de dispositivos, sin que existiera un mecanismo técnico efectivo para impedirlo.

Indicó que, al bloquear un IMEI duplicado, se podía afectar a usuarios legítimos, lo que complicaba aún más la solución del problema. En su caso, reconoció que ni siquiera conservaba la boleta de compra de su teléfono.

Manifestó que existían “puntos ciegos” que merecían ser discutidos. Mencionó que se estaba reportando a una lista internacional de equipos robados para dificultar su exportación, pero advirtió que cada país decidía si bloqueaba o no esos dispositivos. Señaló que países vecinos como Bolivia o Perú podrían no aplicar tales bloqueos.

Alertó que una parte del mercado negro ya no se centraba en la reventa del teléfono completo, sino en la venta de sus piezas, como baterías o pantallas. Comparó los talleres que reciclaban estas partes con “chatarreras digitales” o “aserraderos” para la madera. Indicó que, si bien el Congreso había aprobado una sanción para la adulteración de IMEI, similar a la que existía para el número de chasis de un vehículo, aún no se implementaban mecanismos efectivos para fiscalizar estos talleres, que podían albergar cientos de equipos robados.

Advirtió que tampoco existía control sobre las piezas reutilizadas, que seguían alimentando el mercado negro. Mencionó además el desafío de los teléfonos con múltiples IMEI o con tarjetas SIM electrónicas, lo que obligaría a bloquear múltiples identificadores por aparato.

Reconoció que, aunque se había avanzado, la depuración de la base de datos histórica era difícil debido a la calidad de los datos. Consideró improbable que se pudiera hacer algo con el stock de IMEI repetidos, y abogó por pensar hacia el futuro, desarrollando herramientas de analítica que permitieran detectar patrones sospechosos en el uso de dispositivos.

Sugirió que el software podría alertar cuando un mismo IMEI tuviera múltiples números asociados en un solo día, lo que permitiría identificar teléfonos potencialmente utilizados para fraudes o delitos. Añadió que, al detectar duplicaciones, se podrían implementar mecanismos para que el usuario legítimo fuera identificado y se bloqueara al duplicador.

Finalmente, reiteró la necesidad de revisar la situación de los “chatarreros digitales” y consideró que se debía evaluar si correspondía establecer decomisos u otros mecanismos de control sobre los teléfonos canibalizados para piezas. Afirmó que, aunque un teléfono estuviera bloqueado para operar en la red, sus componentes seguían siendo útiles y comercializables.

****

El señor **Marco Ramírez Álvarez,** , el prefecto jefe Nacional Contra Robos y Focos Criminales de la Policía de Investigaciones de Chile, agradeció a la Comisión por la convocatoria a tratar un tema tan sensible y comentó que, a través de un informe preliminar del análisis realizado por la Policía de Investigaciones, se pudo establecer que el robo de celulares y su vínculo con el crimen organizado evidenciaban que este delito había dejado de ser un delito común. Señaló que se trataba ahora de una actividad ilícita altamente lucrativa y globalizada.

Indicó que estas estructuras criminales operaban mediante diversos delitos como

el robo por sorpresa, con violencia o intimidación, desde lanzazos hasta motochorros, con modos operandi conocidos como "enjambres" o "jaurías". Explicó que el objetivo no era solamente el valor físico del aparato telefónico, sino también el acceso a la información digital contenida en los smartphones, lo que permitía perpetrar estafas mediante aplicaciones bancarias, fraudes, coordinación de secuestros, extorsiones, tráfico de drogas, y otros delitos. Subrayó que estos dispositivos, al ser utilizados como teléfonos desechables, facilitaban evitar la persecución penal y policial.

Ramírez detalló que los mercados criminales operaban en tres niveles: la comercialización de teléfonos nuevos robados, muchos de los cuales eran enviados al extranjero porque el IMEI no podía ser bloqueado; el mercado de teléfonos de segunda mano, cuyo IMEI podía ser adulterado para seguir siendo utilizados; y el mercado de partes y piezas, a través de ferias libres o servicios técnicos encubiertos, que proveían directamente a las organizaciones criminales.

Resaltó que la trazabilidad era un aspecto clave para la localización de este mercado ilegal y explicó que el marco legal que regulaba estos mercados secundarios estaba dado por el artículo 13 de la Ley N° 20.931, el cual otorgaba potestad a la Policía de Investigaciones para exigir actas de procedencia que permitieran identificar el origen de bienes o especies secundarias transadas. Esta trazabilidad permitía detectar delitos, identificar a los responsables y ponerlos a disposición del Ministerio Público.

Asimismo, explicó que el modus operandi incluía el uso de teléfonos nuevos o de segunda mano, utilizados de forma única y luego desechados, para evitar dejar rastros digitales que pudieran vincular a los delincuentes con hechos criminales. Afirmó que el robo de celulares había evolucionado a una actividad ilícita globalmente organizada y lucrativa, con datos que mostraban que no solo se robaba el teléfono, sino que se disponibilizaba en mercados secundarios, y que el valor económico de la información robada variaba según la víctima.

Advirtió que robar el teléfono a una autoridad administrativa o judicial no tenía el mismo impacto que hacerlo a una persona común, lo cual podía derivar en extorsiones o hechos de corrupción, facilitando su vinculación con el crimen organizado. Describió una cadena logística compleja compuesta por roles definidos: quienes cambiaban las piezas, quienes vendían los dispositivos, quienes los transportaban o financiaban, e incluso quienes operaban transnacionalmente. Como ejemplo, mencionó un evento reciente en Perú, donde ciudadanos cruzaban con teléfonos usados al cuerpo.

Indicó que existían investigaciones en curso respecto a ciudadanos extranjeros que venían a comprar teléfonos de segunda mano para comercializarlos en países vecinos, lo cual era enfrentado con equipos especializados de la Policía y del Ministerio Público, con un abordaje territorial e integral. Expuso que esta estructura generalizada nutría los mercados criminales con teléfonos nuevos robados a empresas aseguradas, que eran luego disponibilizados en mercados secundarios tanto nacionales como internacionales.

Añadió que muchos de estos teléfonos provenían de robos con violencia o sorpresa, y que, dependiendo de la demanda, también se diseminaban como partes y piezas. Enfatizó que esta estructura involucraba a múltiples actores: quienes robaban, los servicios técnicos, quienes vendían y quienes venían desde el extranjero a adquirir este patrimonio a un menor costo.

Señaló que esta dinámica generaba una economía circular de oferta y demanda, y que, tal como lo había indicado el Subsecretario, el IMEI dentro del territorio nacional debía ser único y rastreable, por lo que se requería cooperación internacional y un mayor control sobre la venta de equipos de segunda mano. Sugirió que esto debía articularse mediante fiscalización e inspección de actas de procedencia, así como campañas de sensibilización para combatir el comercio ilegal asociado a robos de celulares.

Finalmente, planteó la necesidad de revisar las penas asignadas a estos delitos, ya que muchas veces no se investigaban como delitos complejos (como asociación ilícita o contrabando), sino solo como receptación. Explicó que esa situación

afectaba directamente a los ciudadanos, y por ello recomendó un análisis más detallado respecto a la representación y asignación de penas. Destacó que estos delitos, como el robo por sorpresa y la receptación, se producían diariamente, especialmente en sectores de la Región Metropolitana como Franklin, el Persa Bío Bío o Padre Hurtado. Concluyó que, aunque existían investigaciones complejas que abordaban estructuras criminales completas, también era urgente fortalecer la persecución de los delitos en flagrancia que afectaban diariamente a la ciudadanía.

*****

La señora **Tania Gajardo Orellana**, subdirectora de la Unidad Especializada en Crimen Organizado y Drogas del Ministerio Público. indicó que deseaba compartir una muy breve presentación. Señaló que intentaría no repetir aspectos ya abordados por quien la antecedió en el uso de la palabra. Mencionó que los asistentes podían visualizar la presentación proyectada y que abordaría aspectos que, esperaba, no hubieran sido ya señalados.

Expresó que, desde la Fiscalía, el problema de fondo respecto al robo de celulares iba en la línea de lo planteado por la PDI. Indicó que lo que observaban como fenómeno podía compararse a una pescadería en la cual todo se aprovechaba: la cabeza, el cuerpo del pescado, etc. Afirmó que, en este mercado de celulares, no se desechaba nada. Como lo había indicado la PDI, lo relevante no era únicamente el equipo, sino que ese era sólo una parte del aprovechamiento posible. Se atrevió a afirmar que lo más relevante era el dinero que podía extraerse del teléfono minutos después de haber sido sustraído.

Describió que la primera etapa consistía en la sustracción del aparato, mediante robo por sorpresa, con violencia o intimidación, y que se trataba de organizaciones que, una vez que alguien sustraía el teléfono, lo entregaba rápidamente a otro sujeto. Este último, en general a bordo de un vehículo para no ser fácilmente georreferenciado, conectaba el aparato a un equipo computacional desde el cual se accedía al sistema del teléfono y se comenzaba a realizar transferencias de dinero o pagos con las tarjetas asociadas al dispositivo.

Indicó que en las investigaciones que realizaban dentro de los focos activos relacionados con este tipo de delitos, contaban con información respecto a cómo los sujetos que cometían estos robos estaban alertas respecto al tipo de celular que tenía la víctima, especialmente si se trataba de uno de alta gama, ya que estos estaban vinculados a cuentas bancarias con fondos de los cuales podía disponerse rápidamente.

Detalló que la primera etapa era el robo, seguida por la extracción de dinero desde el teléfono a través de un equipo informático. Luego se utilizaban las tarjetas digitales y, finalmente, se producía la receptación del teléfono, ya fuera en el país o en el extranjero. Insistió en el ejemplo de la pescadería para graficar que en este mercado no se desperdiciaba nada.

Explicó que, antes de la existencia de teléfonos inteligentes conectados a Internet y a bancos, se trataba de tres delitos distintos: el uso fraudulento de tarjeta de pago (anteriormente regulado en la ya derogada ley 20.009), los delitos informáticos (aún vigentes tras la entrada en vigor de la ley 21.595) y la sustracción del teléfono. Indicó que actualmente estos delitos estaban contenidos en el artículo 468 del Código Penal, aunque mencionó que algunas sentencias adversas de tribunales interpretaban que el tipo penal había sido derogado, lo cual representaba un problema.

Reiteró que anteriormente se tenían tres delitos diferenciados: el uso de tarjeta, los delitos informáticos y la sustracción del equipo. Actualmente, con un solo teléfono inteligente vinculado a bancos, un delincuente podía cometer los tres delitos en una sola acción, lo que representaba un incentivo para delinquir. Añadió que con el teléfono se accedía a tarjetas, información bancaria y otros datos que también podían ser utilizados para extorsiones.

Enfatizó que, mientras el fenómeno delictivo había evolucionado, la legislación aún separaba estas conductas. Así, los delitos de sustracción material (robos, hurtos), el acceso indebido informático y el uso de tarjetas estaban regulados de forma

independiente. Esta fragmentación podía implicar que una misma situación fuera investigada como hechos distintos, bajo distintas especialidades tanto en la policía como en la Fiscalía. Señaló que un fiscal especializado en robo no era lo mismo que uno que viera delitos económicos o informáticos.

Expuso que el robo, que antes se consideraba como un delito común, ahora era una actividad altamente lucrativa que constituía un “3 en 1”, y que este fenómeno había tomado por sorpresa a la Fiscalía, la policía, el Estado, la empresa privada y al regulador. Indicó que, aunque se bloqueaban datos como el IMEI, estos podían duplicarse, y que si bien se iban incorporando nuevas medidas —como el bloqueo de tres datos distintos—, siempre el delito iba un paso adelante debido a la alta rentabilidad del mercado. Afirmó que les preocupaba especialmente el cambio fenomenológico, que estaba claramente asociado a organizaciones criminales.

Explicó que no se trataba de individuos aislados, sino de grupos organizados donde cada integrante tenía una función específica: quienes robaban, quienes accedían a los sistemas informáticos, quienes realizaban las compras y transferencias, y quienes vendían o receptaban los aparatos. Añadió que estas organizaciones obtenían importantes ingresos mediante estas actividades.

Indicó que hasta la fecha la Fiscalía había decretado cinco focos investigativos respecto de organizaciones criminales dedicadas a estos fenómenos: en la Región del Biobío, en la Fiscalía Oriente (caso "Enjambre"), en la Región de Valparaíso, en Concepción y en la Región de Los Lagos. Explicó que los focos permitían mejorar la persecución penal al analizar información residual de otras investigaciones y agrupar causas, lo que generaba mejores resultados que mantener los delitos por separado (robo por sorpresa, delito informático, receptación).

Finalmente, expuso una serie de reflexiones y temas que deseaban dejar a conocimiento de la Comisión para ser considerados en futuras mejoras legislativas. En primer lugar, señaló la dificultad de abordar legalmente el fenómeno del “3 en 1” que representaban los teléfonos. Afirmó que el robo por sorpresa no lograba reflejar la gravedad del injusto cuando, además, se accedía a la información del celular y se generaba un perjuicio patrimonial. Indicó que no existía un solo tipo penal que abordara integralmente este fenómeno, sino que seguían vigentes los tipos antiguos, pensados para situaciones de hace 10, 15 o 20 años.

Se refirió a la necesidad de coordinación en casos de flagrancia y geolocalización de teléfonos, tema también vinculado al proyecto de ley de flagrancia en tramitación en el Senado. Indicó que muchas veces no era posible actuar porque no había coordinación entre la policía y la fiscalía, o porque no se cumplían las condiciones temporales de la flagrancia.

Respecto a la receptación, estimó que se podía aplicar un criterio similar al adoptado en los casos de vehículos, donde se había establecido una pena agravada por la relevancia de ese mercado en la delincuencia nacional. Añadió que muchas veces era más sencillo identificar al receptador que a quien sustrajo el aparato.

Por último, comentó que, aunque se había planteado la figura de la “muerte civil” del IMEI, ya había quedado claro que no tenía mucho sentido, dado que los datos podían duplicarse. Concluyó señalando que eso era lo que la Fiscalía podía aportar a la discusión.

****

Habiéndose cumplido el objeto de la sesión, se levanta a las **18.55 horas.**

****

Mario Rebolledo Coddou
Secretario Abogado de la Comisión