COMISIÓN ESPECIAL INVESTIGADORA "OPERACIÓN HURACÁN"

Sesión 12ª, ordinaria, celebrada el día lunes 20 de agosto de 2018.

Se abrió a las 14:02 horas.

SUMARIO:

- Se recibe a los señores Pablo Viollier, analista de políticas públicas de la ONG Derechos Digitales, y Paulo Colomés, ingeniero en redes y experto en seguridad informática.

I.- PRESIDENCIA.

Presidió la diputada señora **Andrea Parra Sauterel**.

Actuó como Abogado Secretario de la Comisión, el señor Álvaro Halabí Diuana; como Abogado Ayudante, el señor Guillermo Díaz Vallejos y, como secretaria ejecutiva, la señora Claudia López Guzmán.

II.- ASISTENCIA.

Asistieron los diputados integrantes de la Comisión, señores (as) Jorge Alessandri, Juan Antonio Coloma, Hugo Gutiérrez, Raúl Leiva, Miguel Mellado, Fernando Meza, Emilia Nuyado, Maite Orsini, Andrea Parra, Joanna Pérez y Osvaldo Urrutia. En reemplazo del diputado señor Torrealba lo hizo el diputado Francisco Eguiguren.

III.- INVITADOS.

Asistieron en tal calidad los señores Pablo Viollier, analista de políticas públicas de la ONG Derechos Digitales, y Paulo Colomés, ingeniero en redes y experto en seguridad informática.

IV.- CUENTA.

- Se dio cuenta de los siguientes documentos:

1.- Oficio N° 14.118, del Secretario General de la Cámara de Diputados, por el cual informa que la Sala, en sesión de fecha 7 de agosto, accedió a la solicitud de prorrogar por 30 días, esto es, hasta el 6 de octubre próximo, el plazo fijado a esta Comisión para el cumplimiento de su cometido.

2.- Correo electrónico del abogado Francisco Ljubetic, por el cual confirma su asistencia a la sesión del día lunes 3 de septiembre.

3.- Reemplazo temporal del diputado Torrealba por el diputado Eguiguren.

4.- Reemplazo temporal del diputado Pardo por el diputado Jorge Durán.

V.- ACUERDOS.

Se adoptaron los siguientes:

1. A proposición del diputado Miguel Mellado, pedir a la Comisión Especial Investigadora sobre SQM la dirección del ex Subsecretario del Interior, señor Mahmud Aleuy, con el propósito de remitirle invitación para la sesión siguiente.

2. A proposición de la Presidenta, oficiar a Carabineros de Chile, a fin de que informe:

a) Cuál es la situación actual de los teléfonos de los generales de la institución en relación con los parches de seguridad que Alex Smith les habría instalado.

b) Respecto del test psicológico al que debió ser sometido don Alex Smith antes de ser contratado por la institución, qué profesional lo realizó y en qué fecha.

3. A sugerencia del diputado Miguel Mellado, solicitar copia del informe en derecho que la ONG Derechos Digitales elaboró para la Defensoría Penal Pública, según lo expuesto por el señor Pablo Viollier.

4. Oficiar a la Biblioteca del Congreso Nacional, a fin de que elabore un informe sobre los estándares técnicos de cadena de custodia de evidencia digital vigentes en la legislación comparada.

VI.- ORDEN DEL DÍA.

A continuación, se inserta la versión taquigráfica de lo tratado en esta sesión, confeccionada por la Redacción de Sesiones de la H. Cámara de Diputados.

TEXTO DEL DEBATE

La señora **PARRA,** doña Andrea (Presidenta).- En el nombre de Dios y de la Patria, se abre la sesión.

El acta de la sesión 9ª queda aprobada.

El señor Secretario dará lectura a la Cuenta.

*-El señor **HALABÍ** (Secretario) da lectura a la Cuenta.*

La señora **PARRA,** doña Andrea (Presidenta).- Sobre la Cuenta, tiene la palabra el diputado Miguel Mellado.

El señor **MELLADO** (don Miguel).- Señora Presidenta, veníamos entrando con el Secretario al Congreso y tuvimos la tremenda sorpresa de encontrarnos con Aleuy en la entrada, por lo que le pregunté en voz alta al Secretario: ¿cómo que Aleuy no está en Chile? Aleuy nos informó que su dirección estaba en su declaración de intereses y patrimonio. Extrañamente, la Comisión de Soquimich lo citó y venía a eso.

Entonces, si efectivamente se ha citado a Aleuy, por favor que se curse la respectiva invitación.

La señora **PARRA**, doña Andrea (Presidenta).- Tiene la palabra el señor Secretario.

El señor **HALABÍ** (Secretario).- Como señalé en la sesión pasada, se han hecho todas las diligencias que han estado en nuestras manos para tratar de invitar al ex Subsecretario del Interior del gobierno anterior, pero ha sido infructuoso.

Como relató el diputado Mellado, su dirección estaría en la declaración de intereses y patrimonio, pero lamentablemente dicha información no es pública.

La señora **PARRA**, doña Andrea (Presidenta).- A fin de despejar el punto, solicito que se pida la dirección a la Comisión Especial Investigadora sobre Soquimich, con el propósito de remitir la correspondiente invitación para la próxima sesión. ¿Habría acuerdo?

Acordado.

Ofrezco la palabra sobre la Cuenta. Ofrezco la palabra.

La presente sesión tiene por objeto recibir al señor Paulo Colomés, ingeniero en redes, y al señor Pablo Viollier, analista de Políticas Públicas de la ONG Derechos Digitales, quienes expondrán al tenor del oficio y de los mandatos que dieron origen a esta comisión.

La sesión tiene una duración máxima de dos horas, por lo tanto, pedimos que acoten sus presentaciones a 20 minutos de exposición, para que luego los parlamentarios realicen sus consultas.

Tiene la palabra el señor Paulo Colomés.

El señor **COLOMÉS**.- Señora Presidenta, primera vez que estoy en una comisión investigadora, así es que agradezco la oportunidad de estar acá.

Mi presentación estará enfocada en explicar las impresiones técnicas que han surgido a través de la Operación Huracán, principalmente a través del software Antorcha, del que todos han escuchado hablar alguna vez. Quiero enfocar el tiempo que tengo en tratar de explicar la forma en que no funciona esta aplicación. Entiendo que el creador de este sistema estuvo en la comisión tratando de explicar cómo funcionaba, por lo que, ahora tengo que hacer lo opuesto. Así es que en virtud del tiempo, avanzaré bastante rápido.

Soy ingeniero informático de la Universidad Católica de Temuco, con más de 15 años de experiencia en el área de comunicaciones de red, comunicaciones y seguridad, y tecnologías de la información, así es que es una materia en la que me

manejo. Entiendo de qué se trata y las cosas que pueden y no pueden ser cuando se habla de temas técnicos.

Esta presentación tiene por objeto hacer un breve análisis técnico de la aplicación Antorcha, desde el punto de vista técnico, pero no profundo, sino más bien con lenguaje simple para que se pueda entender. Lo mismo haré con la otra aplicación, que también tiene relación con este caso, denominada Tubicación.

Respecto de si es posible interceptar WhatsApp u otras aplicaciones de mensajería instantánea, lo explicaremos y daremos un par de conclusiones.

La Unidad de Inteligencia Operativa Especial (U.I.O.E.) de Carabineros, con sede en Temuco, aseguraba que, mediante algunas aplicaciones informáticas desarrolladas en esa unidad, era posible lograr la intervención de aplicaciones de mensajería instantánea.

Lo primero que llama la atención es el universo de aplicaciones involucradas. Mucho se habla de Whatsapp, pero también han aparecido Telegram, tecnologías de Iphone, Android, Gmail, Facebook y Twitter, que son sistemas muy conocidos y grandes empresas a nivel mundial, con muchos recursos, los cuales son invertidos en implementación de sistemas de seguridad. Por eso, llama la atención que esta supuesta aplicación tenga un espectro tan amplio de acción, con tantas aplicaciones.

Principalmente, este software aseguraba interceptar las comunicaciones, pero ya se demostró lo contrario en un peritaje de la Policía de Investigaciones, en mayo de este año. Hay bastantes antecedentes al respecto. Creo que el peritaje consta de 200 hojas, que si bien están en lenguaje técnico, se pueden consultar. En definitiva, ya se estableció que el software no funciona, pero como puede ser un poco más técnico, me enfocaré en una presentación más sencilla, con un lenguaje más cotidiano.

En cuanto a lo que planteó el señor Smith respecto de la forma en que funcionaría la aplicación que permitió ser usada para apresar a ocho comuneros mapuches mediante la extracción de mensajes de mensajería instantánea, en primer lugar, esta persona decía que la aplicación consistía en un espejo del teléfono. Siempre se mencionó que se utilizaba un espejo, pero más allá de esa explicación, nunca hubo algo más detallado. ¿Qué es realmente un espejo? ¿En qué consistía la explicación?

Asimismo, decía que la aplicación Antorcha se abría en el computador y debían ingresarse datos como el correo electrónico, el IMEI, la *simcard, el* número del chip telefónico, pero tampoco se dio una explicación de por qué ni para qué se necesitaba un IMEI o un *simcard.*

Supuestamente, el servidor instalado en las dependencias de Carabineros de Temuco enviaba un correo electrónico al teléfono que se quería intervenir. Por ejemplo, si tenían un "blanco", como lo llamaban, enviaban un correo electrónico a esa persona, llegaba al teléfono y ese correo contaminaba el teléfono. Para los que trabajamos en esta área es algo sospechoso, por lo que me encantaría saber cómo sucede, fue una de

las primeras cosas que a mucha gente de la comunidad de seguridad y ciberseguridad en Chile llamó la atención.

Luego, empezamos a ver la fantasía, la ciencia ficción, porque se aseguraba que bastaba que el correo llegara al teléfono para infectar el aparato, no era necesario verlo, sino que simplemente con el hecho de que llegara al correo ya podrían interceptar las comunicaciones.

Como decía, no era necesario que el usuario, la víctima, abriera el correo electrónico que se le había enviado, solo bastaba con que ingresara para ver esa información en otro aparato. Específicamente hacen referencia a Whatsapp y Telegram.

Otros alcances: Se compraron varios dominios, por ejemplo, Airs.cl y Tubicacion.cl, que todavía están en funcionamiento. Incluso, si alguien los quiere ver pueden ingresar y se darán cuenta de que no hacen nada, es una simple plantilla, una página web común y corriente que no tiene funcionalidad alguna.

El señor Smith en numerosas ocasiones cambió la versión de la forma en que funcionaba su aplicación. En distintas oportunidades, como representante de la comunidad de ingenieros, tuve mucho interés en entender cómo podía funcionar realmente; incluso, me sentí muy decepcionado cuando supe que nunca se logró explicar con sustento el funcionamiento de Antorcha. También lo explicó en televisión y en esta propia comisión, por lo que ustedes han sido testigos de primera mano de que no funciona.

Otra cosa que nos ha llamado la atención es que todas las pruebas se han hecho en un teléfono Android y usando un Gmail, pero nunca se ha utilizado ni mencionado un teléfono iPhone.

Tampoco se ha entregado información que permita, por ejemplo, reproducir el funcionamiento en un entorno de prueba: ver cómo funciona, tomar la evidencia y hacer lo mismo en mi casa como experto. Eso no es posible, no existe. El señor Smith nunca permitió que su aplicación fuera analizada por expertos en un entorno controlado, en una universidad o en un entorno imparcial. Es más, en algún momento quiso ir a Estados Unidos para que el FBI analizara la aplicación, lo que francamente es ridículo porque hoy existen soluciones informáticas muy avanzadas que hacen cosas más espectaculares de las que eventualmente podría haber hecho Antorcha y nadie necesita ir al FBI para demostrar que funcionan. Basta entrar a un canal de YouTube para que le expliquen cómo funciona y con eso es suficiente.

Existen sitios web especializados en internet para subir un *paper* y explicar la forma cómo funciona, y parte de los códigos fuente los puede tener disponibles para que la comunidad completa valide que se trata de algo legítimo. Por tanto, no es necesario ir al FBI, porque este último necesitaría un departamento específico destinado a recibir gente que inventa cosas. Insisto, a mi juicio, no es necesario y absolutamente ridículo. Además, los peritajes de la PDI ya establecieron la falsedad de la aplicación.

Ahora bien, una de las aristas más importantes durante el transcurso de lo que ha sido la Operación Huracán fue la

presentación en un canal de televisión donde se le dio la oportunidad al señor Smith de presentar su aplicación y la población en general quedó con la impresión de que realmente podría funcionar. Al respecto, quedaron muchas dudas porque el reportaje no fue claro ni categórico en decir si funcionaba o no.

Por ello, les quiero mostrar un par de cosas puntuales para que vean por qué no funciona. En la imagen pueden ver una captura de pantalla -abajo aparece el *link*, el video todavía está disponible en el sitio del canal de televisión- en la que mostraba su *software*, pero se puede apreciar que en el *slide* izquierdo, en la parte superior, hay una cinta de color blanco que oculta algo. Lo que oculta es la dirección del sitio real: Xploitz.net, un sitio común y corriente al que cualquier persona de hasta 10 años de edad puede entrar y *hackear* un Facebook. Lo que este hace es preparar una plantilla con la imagen falsa de Facebook -los famosos ataques de *phishing* que se envían por correo-, basta entrar, no hay que hacer nada y el sitio lo crea; eso es todo. Entonces, se presentó Antorcha como esto, pero es un sitio *web* gratuito que cualquiera puede visitar.

Después de ver esto en televisión, pensamos que era francamente ridículo, como dije en un comienzo.

La señora **PARRA**, doña Andrea (Presidenta).- Entonces, el señor Alex Smith nos mintió descaradamente, porque aparte de cambiar sus versiones constantemente, como lo hizo muchas veces en esta mesa, debemos estar conscientes de que ese sitio existía y él estaba mintiendo.

El señor **COLOMÉS**.- Para mí es asombrosa su capacidad para mentir. No sé por qué lo hace, pero hay un hecho concreto de que eso no es Antorcha, es un sitio *web* que está en internet y cualquiera lo puede usar, no tiene ninguna ciencia.

Ese mismo programa de televisión -como señalé lo pueden ver en el *link*- consta de dos partes. La primera se enfoca en tratar de interceptar un mensaje para reproducir lo que eventualmente hubiera ocurrido en la Operación Huracán. Incluso, el periodista escribe un texto a una colega, el que muestra la imagen, extraído del mismo video, pero lo concreto es que en el resultado del programa nunca se mostró que ese texto fuese interceptado. Lo que posteriormente se hizo fue dar una explicación de que se demoraba mucho, que se estaba incubando, etcétera, es decir, una serie de cosas extrañas. También denunciaron que le *hackearon* el sistema.

La exabogada del señor Smith, Marisa Navarrete, participó en la segunda parte del reportaje, y prestó su propio celular para que pudieran interceptar las comunicaciones. Se mostró que se capturaron algunas fotos que fueron recibidas por Whatsapp y eso fue real, por ello quiero aprovechar la oportunidad para señalar que eso tiene una explicación muy sencilla.

Las personas que tienen teléfonos Android tienen la opción, no siempre, de hacer un respaldo automático de las conversaciones y fotos de Whatsapp en la nube de Google. Si

tiene un correo Gmail -por eso este señor siempre les pedía un Gmail- se sube a una nube donde se almacenan dos cosas: las conversaciones de Whatsapp y las fotos. La diferencia está en que las conversaciones están cifradas, no se pueden recuperar. No hay ninguna manera de que descargando ese archivo pueda ver las conversaciones, están protegidas por un mecanismo criptográfico bastante avanzado. Lo que se pueden ver son las fotos, porque no se almacenan cifradas, sino tal como están.

El señor **GUTIÉRREZ**.- ¿Las fotos pueden verse?

El señor **COLOMÉS**.- Sí, así es. Cuidado con lo que guarda y con lo que recibe, porque en Whatsapp existe la opción de guardar todo lo que recibe. En mi caso no guardo nada de lo que recibo a través de esa aplicación.

Entonces, si logro obtener su clave de Gmail y sé que su celular se sincroniza con esa nube, basta con entrar a su cuenta de Gmail y puedo bajar sus fotos de Whatsapp, porque se almacenan sin cifrar, pero eso no se puede hacer con las conversaciones.

Les voy a dejar el link a un video en Youtube que dura 35 minutos, pero no es para que lo vean ahora. En un día muy aburrido de febrero en nuestra oficina, con un colega decidimos replicar ese funcionamiento y tratar de hacer que funcionara Antorcha. Hicimos todas las pruebas técnicas posibles y determinamos que sí se podían obtener las fotos, pero no las conversaciones. Al menos yo, en mi experiencia, no conozco una manera de obtenerlas a través de un respaldo, y muchos colegas del área coinciden en ello. Las conversaciones se almacenan en un formato especial, distinto al de texto; se almacenan en una base de datos que es bastante complicada de manipular, de modo que, desde un punto de vista técnico, no es tan sencillo como se decía. En el video que les mencioné está la explicación, dura 35 minutos. Si alguien tiene tiempo, puede verla.

Como conclusión de este reportaje, jamás se obtuvo la conversación inicial, eso no sucedió. Se explicó que había un virus incubando en el sistema operativo, pero no se dieron muchos detalles de eso, simplemente se dijo que falló porque había un virus. Es la explicación más sencilla que se puede dar cuando algo no funciona.

También se dieron otras explicaciones, como, por ejemplo, que lo habían hackeado durante la noche, alguien del centro de Santiago, y varias explicaciones muy extrañas.

Nunca se mostró cómo realizar este procedimiento en un teléfono Iphone, solo en un Android, porque eventualmente sería más sencillo. Tampoco se ha explicado cómo se podrían recuperar las conversaciones de Telegram. Sí se mencionó, en un principio, que esa aplicación recogía los datos de Telegram.

El señor **GUTIÉRREZ**.- ¿Es más fácil hacerlo en Android?

El señor **COLOMÉS**.- Sí, porque el Iphone tiene un mecanismo de seguridad muchísimo más avanzado que el de Android y

es mucho más difícil "poner un virus" en un teléfono Iphone. No digo que sea imposible, pero es mucho menos probable. En cambio, en el Android es un poco más fácil porque es más manipulable.

Como les decía, en ese reportaje, la exabogada del señor Smith presentó su teléfono para que pudiera validar ese procedimiento, algo bastante conveniente, pero sigo insistiendo en que esa aplicación es un total fraude. Nunca alguien ha podido demostrar que realmente funciona, ni el mismo creador.

Aparte de Antorcha, también salió una aplicación llamada Tubicación, que es menos famosa, pero también figura en la Operación Huracán 2. La justificación de esa aplicación, creada también por el señor Smith, era que permitía georreferenciar los teléfonos de las personas a partir de una señal de *router* wifi común y corriente, como los que tenemos en las casas, y de esa manera identificar el teléfono de alguien. De hecho, entiendo que esa fue la justificación para identificar a los responsables del ataque de los 29 camiones en San José de la Mariquina. Eso es una vergüenza, es imposible, no tiene ningún sustento, es un invento, es totalmente una fantasía, es un fraude.

Eso es muy sencillo de entender. En este caso, la justificación fue que, como la empresa que sufrió el atentado tenía un *router* que emitía una señal, se perició ese dispositivo y de allí se obtuvieron los números de teléfono de esas personas, así entiendo que sucedió.

Todos los teléfonos celulares -y los computadores, de hecho, pero los teléfonos celulares, principalmente- tienen, entre todos los identificadores o códigos de identificación, dos que se llaman Dirección Mac y Dirección Imei. La dirección Mac sirve para identificarse en una red wifi y la dirección Imei es para hacerlo en una red de celular, son dos cosas separadas.

Dentro del teléfono, esos mecanismos están aislados y no tienen comunicación unos con otros. En el fondo, no hay ninguna manera de que alguien identifique mi número telefónico valiéndose de una red wifi. Eso no se puede hacer, son sistemas totalmente distintos. Sería como explicar, por ejemplo, que si usted me da su número de teléfono, yo le puedo decir cuánto calza. ¿Habrá alguna forma? No tengo idea. No tiene relación una cosa con la otra. En consecuencia, esa justificación es totalmente falsa, eso no es posible, no se puede determinar un número de teléfono a través de una conexión.

Además, para dar algo de credibilidad a esa historia, habría que pensar que las personas que entraron a incendiar esos camiones deberían haberse conectado a la red wifi, pero creo que, si están quemando camiones, lo último que pensarían sería conectarse a internet y, además, tendrían que saber la clave. Si fuera por eso, siempre que pasara por un lugar con una red wifi abierta sabrían que yo ando ahí, porque mi número de teléfono quedaría registrado, pero eso no es así. Tal aseveración podría servir como base para el guión de una serie de Netflix, pero eso no ocurre en la realidad.

La forma en que efectivamente se pueden georreferenciar teléfonos celulares y encontrar personas es muy simple y se

ocupa frecuentemente. Ello se sustenta en que las compañías de telefonía celular tienen la tecnología necesaria para triangular la señal que emiten los teléfonos y determinar que alguien estuvo usando la señal de tres o cuatro antenas de un determinado punto. Con esa técnica se puede llegar a una referenciación parcial, de entre 500 metros a 4 kilómetros, dependiendo de la zona donde se utilice. Eso sí es mucho más factible. Entonces, bastaría con haber ido a las compañías proveedoras del servicio y preguntar si un usuario identificado con un número telefónico estuvo o no en un determinado lugar.

No sé si legalmente corresponde hacer eso -mi colega podrá explicarlo después-, pero técnicamente sí se puede hacer. Cualquier compañía puede saber dónde está usted en este momento, a través de este sistema.

El señor **LEIVA**.- ¿Llame o no llame?

El señor **COLOMÉS**.- Llame o no llame, porque todo el tiempo está conectado a alguna celda. Con el teléfono celular usted se desplaza y se conecta a una torre con cierta intensidad y también a otra con menor intensidad.

El señor **GUTIÉRREZ**.- ¿Y si el teléfono celular está apagado?

El señor **COLOMÉS**.- Si está apagado, no hay forma de rastrearlo.

El señor **GUTIÉRREZ**.- Solo se hacen llamadas.

-Varios señores diputados hablan a la vez.

La señora **PARRA**, doña Andrea (Presidenta).- Señores diputados, para efectos de orden, les solicito pedir la palabra antes de intervenir.

Señor Colomés, para hacer ese rastreo, ¿la persona debe tener prendido su celular?

El señor **COLOMÉS**.- Por ejemplo, en este momento estoy conectado a la red de mi compañía de teléfonos y ellos pueden saber que estoy en el centro de Santiago, no en Temuco. Eso lo pueden saber en este momento porque mi teléfono está conectado a la red celular. Está generando una señal 3G o 4G, pero no es necesario que esté haciendo una llamada. Podrían saberlo, porque tienen los mecanismos técnicos para hacerlo.

El señor **GUTIÉRREZ**.- Señora Presidenta, una consulta. Se suele decir que, aún cuando un teléfono celular esté apagado, es posible detectar dónde está la persona que lo porta. ¿Eso es cierto? ¿Es mitología?

El señor **COLOMÉS**.- Creo que eso es mito. No tengo forma de entender cómo algo que no está con energía podría ser usado para tal tipo de detección.

El señor **GUTIÉRREZ**.- Cuando está en modo avión, ¿tampoco se puede rastrear?

El señor **COLOMÉS**.- Tampoco, porque el modo avión apaga las antenas wifi, Bluetooth y de red celular.

La señora **PARRA**, doña Andrea (Presidenta).- Tiene la palabra el diputado señor Raúl Leiva.

El señor **LEIVA**.- Señora Presidenta, me dirijo por su intermedio a nuestro invitado.

Como usted bien dice, estando conectado a la compañía de teléfonos, es posible ubicar a una persona por medio de su celular. ¿Qué respaldo tienen y cómo pueden ubicar de aquí en adelante, o existe un *backup*, un registro hacia atrás de las compañías?

El señor **COLOMÉS**.- Lo desconozco, pero entiendo que las compañías de teléfonos llevan un registro, creo que hasta por dos años. Para ser preciso, no tengo esa información. No sé cuánto podrá ser.

El señor **VIOLLIER**.- Señora Presidenta, ¿puedo responder?

La señora **PARRA**, doña Andrea (Presidenta).- Por supuesto.

Tiene la palabra el señor Viollier.

El señor **VIOLLIER**.- Señora Presidenta, eso es parte de lo que se denomina metadatos de comunicaciones. El metadato, como indica su nombre, es un dato sobre un dato.

El artículo 222 del Código Procesal Penal obliga a las empresas de telecomunicaciones a guardar un número de direcciones IP de las conexiones de sus abonados. Eso significa que las empresas de telecomunicaciones no guardan nuestras comunicaciones, como mensajes de Whatsapp o correos electrónicos, pero sí los números de conexiones IP de nuestras conexiones.

Son muchos datos. De hecho, fue parte de lo que combatimos el año pasado y que denominamos como decreto espía, que fue un intento del entonces subsecretario del Interior del último gobierno de Michelle Bachelet, Mahmud Aleuy, de extender ese almacenamiento de datos de un año a dos años. Ese almacenamiento es de datos de telecomunicaciones.

Por lo tanto, las compañías saben, por ejemplo, que lo llamé a las 14 horas, que estaba conectado –está muy bien presentado ese gráfico-, que llamé a tal número, que la llamada tuvo una duración de 3 minutos y que estuve conectado a tales y tales antenas.

Como ven, no se trata del contenido de la comunicación, sino de los datos. Es como una carta que tiene registrado el remitente, el emisor y los lugares por los que pasó. El dato es alrededor de la comunicación.

El señor **LEIVA**.- Es como el registro de llamadas.

El señor **VIOLLIER**.- Exactamente. Esos son los datos que las compañías tienen la obligación de almacenar por al menos un año y, justamente, como bien dice Paulo, es lo que se puede utilizar para tener la ubicación aproximada, porque si una persona llamó y la triangulación fueron estas tres antenas que están en el centro de Santiago, sabe que esa persona en tal fecha estuvo en el centro de Santiago.

Nos opusimos a la extensión de la retención porque si se realiza un análisis de todos esos datos comunicacionales puede saber dónde estuvo esa persona, ver su rutina, con quién se comunica, quiénes son sus pares, si llamó a una línea de una clínica de aborto o a una de suicidio.

Entonces, se puede saber mucho a partir de esta información, que son metadatos. En este caso la ubicación solo puede ser a través del registro que manejan las ISP.

Para tener acceso a esa información se requiere una autorización judicial al interior de un proceso penal. Es decir, es la información que las compañías almacenan por un período no menor a un año y que entregan con una orden judicial dentro de un proceso de investigación penal.

El señor **LEIVA**.- Señora Presidenta, solicito la palabra.

La señora **PARRA**, doña Andrea (Presidenta).- Tiene la palabra su señoría.

El señor **LEIVA**.- Señora Presidenta, quiero realizar una última pregunta sobre algo que me pareció interesante.

¿Se trata solo del registro de que llamó a tal hora y, eventualmente, a través de la dirección *email* de tal lugar? ¿Y las comunicaciones?

El señor **VIOLLIER**.- No. Como señalé, es el dato comunicacional. Es la información sobre la comunicación, pero nunca del contenido de la comunicación. De hecho, las empresas de telecomunicaciones no tendrían la capacidad para almacenar el contenido, porque cada llamada son archivos grandes por el contenido de los mensajes.

Es información que las empresas guardan para la entrega del servicio de telecomunicaciones, pero puede ser utilizada eventualmente dentro de investigaciones penales, como por ejemplo, decir: yo vi que estuviste llamando a tal persona y esa persona fue la que te compró la droga.

Inicialmente, la ley obligaba a almacenar esta información por un período de 6 meses, después se extendió a un año para efectos de investigación penal, pero, insisto, no es el contenido de la comunicación, sino el remitente, el emisor, la fecha, la duración de la llamada, etcétera. Por ejemplo, dentro de la página *web* me conecté a tal IP que corresponde a la página *web* Xploitz.net. Repito, no es el contenido, sino el dato comunicacional.

La señora **PARRA**, doña Andrea (Presidenta).- Tiene la palabra el diputado señor Miguel Mellado.

El señor **MELLADO** (don Miguel).- Señora Presidenta, pido a alguno de los invitados que nos grafique cuál es la forma de pinchar los teléfonos, intervenirlos, y escucharlos.

Invitados a la comisión presentaron al juez Aner Padilla una lista de personas a las cuales se podía pinchar sus teléfonos y escuchar sus conversaciones. ¿Saben ustedes cómo se hace eso?

La señora **PARRA**, doña Andrea (Presidenta).- Tiene la palabra el diputado señor Hugo Gutiérrez.

El señor **GUTIÉRREZ**.- Señora Presidenta, quiero saber si es posible respecto de ese metadato, por ejemplo, en virtud de la denominada Ley de Inteligencia, que se pida a las mismas empresas que pinchen el celular y graben la conversación. ¿Se puede pedir eso?

¿Es posible que den a conocer los datos de la persona a quien llamó y que graben las llamadas que realizó desde su celular esa persona durante todo ese año a través de la denominada Ley de Inteligencia, con solicitud al ministro de la corte y todo lo que corresponda?

La señora **PARRA**, doña Andrea (Presidenta).- Tiene la palabra el señor Paulo Colomés.

El señor **COLOMÉS**.- Señora Presidenta, la pregunta del diputado Mellado solo la puedo responder parcialmente, porque no tengo el detalle exacto. Un experto que trabaje directamente en las compañías de telecomunicaciones tiene más detalles, pero si un juez eventualmente dicta la orden de intervenir un teléfono celular, y se entrega esa información a una compañía, no veo que haya una limitación técnica para decir que no se puede hacer. Personalmente, no conozco una limitación técnica. Se usan *software* y máquinas. En realidad, hoy en día todo es *software*.

Una señora **DIPUTADA**.- ¿Por qué el software podría intervenir la comunicación telefónica y no el WhatsApp?

El señor **COLOMÉS**.- Porque son canales de comunicación diferentes. Una cosa es la voz que tengo en el celular, que se codifica de una manera determinada para que viaje por las señales del celular a través de voz y otra cosa son los datos de internet, que tienen otros mecanismos de protección adicional, por ejemplo, un cifrado.

La dirección de una página web que comienza con *https*, como las de los bancos, tiene un sistema de seguridad adicional que permite que nadie espíe la comunicación.

El señor **MELLADO** (don Miguel).- ¿Cualquier persona puede pinchar un teléfono o debe ir a la compañía para sacar de ahí los datos?

El señor **COLOMÉS**.- En ese contexto diría que prácticamente es imposible que alguien pueda pinchar el teléfono de otra persona. Podría haberse hecho hace 20 años, cuando los

sistemas celulares eran bastante vulnerables y había formas de hacerlo. No podría decir que es imposible, pero estos sistemas han evolucionado de tal manera que es muy poco probable que alguien lo pueda hacer.

Sin embargo, lo común es que la compañía telefónica lo pueda hacer, porque es el punto de terminación de la llamada telefónica.

La señorita **ORSINI** (doña Maite).- Entonces, ¿hay un *software* que permite hacerlo? Por algo Carabineros, y dicen por ahí que también Fiscalía, tienen una máquina. Si ellos la tienen, ¿otra persona podría comprar ese *software* afuera, traerlo y usarlo?

El señor **COLOMÉS**.- Desconozco eso, y creo que no. En la forma en que funcionan las telecomunicaciones me atrevería a decir que eso solo lo puede hacer alguien que tenga acceso a la terminación de la llamada, es decir, la compañía telefónica, pero no un tercero.

El señor **LEIVA**.- Intervenir por el aire, sin tener acceso al aparato telefónico, es muy complejo.

El señor **COLOMÉS**.- Casi imposible.

El señor **LEIVA**.- Pero si usted tuviera eventualmente acceso a mi dispositivo celular, ¿sí se puede intervenir?

El señor **COLOMÉS**.- Se puede. Lo voy a explicar. La pregunta más común que ha surgido acá es si es posible "hackear el *WhatsApp"*, y lo pongo entre comillas porque simplemente es espiar una comunicación. La verdad es que se puede. Hay varias formas de que una persona pueda tener acceso a la comunicación de *WhatsApp* de otra persona, pero para eso se deben cumplir una serie de requisitos. No es tan fácil como decir que tengo su número. No es tan sencillo.

En primer lugar, hay que tener acceso físico al teléfono y conocer la clave. En los teléfonos con sistema operativo *Android* es muy fácil porque la grasa de los dedos queda marcada en el patrón de desbloqueo. Entonces, si se mira a contraluz es muy fácil.

En el video que indiqué demostramos con un colega que en cinco minutos se puede intervenir el teléfono para sacar las claves y, eventualmente, ver las fotografías almacenadas. O para instalar una aplicación, por ejemplo, una llamada Mspy y otras que funcionan bastante bien y que se pueden instalar en el teléfono porque el equipo entiende que soy el dueño legítimo. Básicamente, lo que puedo hacer es tener una conversación viéndose en otro lado, pero debo tener acceso físico al dispositivo y el tiempo necesario para hacer todo lo que he indicado. Hay que tener la clave de acceso y una serie de otras cosas.

La otra opción es aplicar un *software* forense, avanzado, profesional, como *Oxygen Forensic*, bastante conocido, no es muy barato, pero puede hacer algunas cosas. Esa es tecnología forense.

Una manera de hacer esto en forma remota es robándome los datos del sistema de almacenamiento iCloud, si tiene iPhone, o robándome los datos Gmail si tiene un dispositivo Android.

En ese caso hay dos vectores de ataque. Primero, ingresar al teléfono directamente si no tiene una protección llamada autenticación de doble factor. Si su teléfono no la tiene, por favor habilítela. Si alguien quiere ingresar a su cuenta, aun cuando tenga las claves, le va a mandar un mensaje de texto. Por ejemplo, me robo los datos de su aplicación de correo electrónico Gmail, y si usted usa un dispositivo Android puedo intervenir su teléfono, sacar sus fotos, etcétera.

Si no tiene habilitado el sistema de autenticación de doble factor simplemente voy a acceder a esa comunicación, pero si tiene habilitada la opción el sistema va a mandar un mensaje de texto a su teléfono que tengo que ingresar para validar que tengo el teléfono en la mano. Es una segunda clave.

-Hablan varios señores diputados a la vez.

Es la misma aplicación de WhatsApp. En Gmail se puede hacer. Instagram lo soporta, también Gmail, todas las plataformas soportan la autenticación doble. Les recomiendo que la activen.

Segundo, la última opción posible, pero muy recontradifícil, sería que alguien pudiera crear una aplicación pirata, entrecomillada Antorcha, por ejemplo, subirla al sistema de *Google Play* y desde ahí infectar un teléfono. Eso es factible, pero muy difícil. Y en el transcurso de toda la "Operación Huracán", nunca se ha mencionado siquiera esa opción.

La señora **PARRA**, doña Andrea (Presidenta).- Tiene la palabra el diputado señor Fernando Meza.

El señor **MEZA**.- Señora Presidenta, conozco la capacidad de nuestro invitado, quien es de mi zona, y también de sus colegas.

¿Cree usted que Carabineros de Chile tiene personal capacitado para hacer este tipo de intervenciones, este tipo de hechos, conocido como la "Operación Huracán", desde el punto de vista técnico? ¿Existen esos especialistas allí?

El señor **COLOMÉS**.- En verdad, desconozco si internamente Carabineros tiene gente capaz de hacer eso. Sería irresponsable de mi parte decir sí o no.

Lo que puedo decir es que en Chile sí hay gente capacitada para hacerlo. Son pocas, pero existen. Sin embargo, no tengo los conocimientos para decir si Carabineros tiene o no esa facultad.

La señora **PARRA**, doña Andrea (Presidenta).- Tiene la palabra el diputado señor Raúl Leiva.

El señor **LEIVA**.- Tal como lo planteaba el diputado Fernando Meza, quiero saber si existe un perfil académico y técnico dentro de Carabineros como para realizar esto. Obviamente, usted respondió que no sabía.

Entonces, ¿cómo Carabineros, teniendo ingenieros informáticos, técnicos en programación o analistas de sistemas no fue capaz de desvirtuar lo básico, entrecomillas, de "Antorcha"?

El señor **COLOMÉS**.- Entiendo que esto sucedió a través de una "ley de Inteligencia" que no permitía publicar mucho dentro de la misma rama de Carabineros. Entiendo que fue así. Eso puede ser una explicación.

Pero creo que no solo Carabineros, sino todas las Fuerzas Armadas, y casi todos los estamentos públicos, debiesen contar con gente, con un departamento o con alguien que esté capacitado para hacer de contraparte cuando suceda algo como esto.

El señor **LEIVA**.- Pero uno entendería que, cuando es algo más sofisticado, uno requeriría un rigor académico técnico mayor. Pero lo que muestra Pablo Viollier, y que me llama profundamente la atención, es que era demasiado básico, como para que ningún técnico en computación no haya...

El señor **COLOMÉS**.- No sé qué otra persona calificada tuvo acceso a ese *software* o a esta situación cuando estaba sucediendo. Pero, cuando apareció en televisión, el comentario general fue que esto era un chiste.

El señor **LEIVA**.- Quisiera hacer una segunda y última pregunta, aprovechando su capacidad técnica.

Usted bien planteaba que teniendo acceso físico al teléfono y teniendo las claves, un experto en informática puede hacer lo que quiera.

El señor **COLOMÉS**.- No sé si lo que quiera, pero...

El señor **LEIVA**.- Replicar la información, interceptar comunicaciones. No solo datos, sino también diálogos.

Conforme hemos entendido, y sabido en esta Comisión, el año pasado, o antepasado, cada uno de los generales de Carabineros entregó su dispositivo y sus claves a disposición del señor Smith, para que, entre comillas, se instalara un parche.

Por lo que explica, entiendo que, teniendo a su disposición el acceso físico y a las claves del teléfono, uno podría replicar todo, intervenir todo o monitorear todo lo que pasa en ese aparato.

Si ese parche se mantuviera, como nos dijo hoy el director de Inteligencia, ¿podría tener acceso a esa información cualquier persona?

El señor **COLOMÉS**.- No sé si cualquier persona, pero si ese parche fuese una aplicación legítima, eventualmente sí. Podría ser.

-Hablan varios señores diputados a la vez.

El señor **VOILLIER**.- Son situaciones altamente irregulares. Ningún asesor informático le pediría a algún cliente que le diera acceso de esas características a las cuentas personales de una figura pública. Eso es altamente irregular.

El señor **LEIVA**.- Ya, pero teniendo claro que eso sucedió ¿qué recomendaría técnica y jurídicamente respecto de esos aparatos de cada uno de los generales de Carabineros?

El señor **COLOMÉS**.- Yo recomendaría un peritaje informático profesional a alguna de las empresas conocidas del rubro, nacional o internacional, que pueda determinar si lo instalado ahí fue algo inexistente o es un *software* espía. Pero sí se puede hacer, o establecer, a través de un peritaje forense. Recomendaría técnicamente eso.

La señora **PARRA**, doña Andrea (Presidenta).- Tiene la palabra el señor Mellado.

El señor **MELLADO**.- Dado lo que estaba diciendo recién el diputado Leiva, quiero recordarles que este *software,* "Oxygen Forensics", fue comprado con plata del fondo reservado los primeros días de septiembre. Y el parche fue colocado después, para este *software* avanzado, no llegue a los celulares de los generales.

Entonces, si nos puede explicar en castellano puro ¿qué hace este *software* forense avanzado? ¿Qué lo hace tan peligroso, que causó miedo dentro de la gente que estaba en la unidad operativa y que hizo proteger a los generales de Carabineros?

El señor **COLOMÉS**.- Lo que pasa es que, a través de un análisis forense profundo, se puede obtener mucha información. Hay alguna información que no se puede obtener. Cosas que están protegidas por mecanismos criptográficos, no se pueden obtener, pero otras cosas que están sueltas si se pueden obtener. Por ejemplo, archivos que han sido borrados, sitios web que se han visitado anteriormente y que también fueron eliminados. Cosas como esas. Se puede obtener mucha información: contraseñas, claves de correos, de bancos, etcétera. No diría que el ciento por ciento de las cosas, pero sí mucha información se puede obtener a través de un análisis forense.

El señor **MELLADO**.- ¿Siempre con acceso físico al teléfono?

El señor **COLOMÉS**.- Si, siempre con acceso físico al teléfono. Remotamente, casi imposible.

Y para terminar esto, ahí les tengo mi "Antorcha" 2.0. Lo pueden hacer ustedes en un sitio web, que se llama hackear correos. Esto es lo que hizo es Alex Smith. Buscó un sitio en internet que decía: Vamos a hackear *key-mails*; eso busqué yo. Y básicamente hizo el show en base a lo mismo. Así que, si a

alguien le interesa, puede meter su número de teléfono ahí y no pasa nada.

Bueno, mi conclusión al respecto, como dije, es que esta aplicación no existe, nunca existió. La PDI también determinó lo mismo, a través de su análisis. No tenía acceso a eso, pero me he basado en lo que ha aparecido en los medios. En el mejor de los casos, esto podría tratarse simplemente de un procedimiento, no de una aplicación como tal, no un *software* con código, sino un procedimiento, pero tampoco eso garantiza efectividad.

Por otro lado, la aplicación "Tubicación" no solo no existe, sino que es un fraude total. También queda demostrado ampliamente y documentado que las aplicaciones de informática que dieron sustento a esta operación, carecen de los mínimos requerimientos técnicos para incluso ser consideradas como posiblemente factibles. Ni siquiera da para eso.

Entonces, en mi opinión, a lo mejor esta persona, la información que empezó a publicar, la obtuvo de otras fuentes que tal vez no eran legales. Pero sí la obtuvo porque trabajó en Inteligencia de Carabineros y ahí uno puede recibir más información que cualquier mortal. A lo mejor, la información sí se obtuvo de otros medios, pero no de una aplicación que intervenía los teléfonos y toda esta fantasía.

Cabe destacar que esta situación es insólita en Chile, porque los países industrializados cuentan, en sus gobiernos, el Estado como tal, con personas contratadas para temas de *hacking* para asesoramiento, y que tiene como objetivo proteger intereses nacionales. Algunos países son un poco más ofensivos y van a atacar a otros. Pero la mayoría de los países tienen sus mecanismos internos de protección.

También las policías cuentan con un alto grado de especialización en el tema de seguridad informática, lo que les permite, por ejemplo, discernir si una cosa como esta puede ser verdad o no. Las policías están preparadas para eso.

Mi última conclusión es que si Carabineros hubiese tenido, por ejemplo, un grupo de esta índole, tal vez los verdaderos culpables ya estarían procesados, porque las evidencias que se podrían haber recopilado sí hubiesen pasado la prueba de un análisis forense común y corriente.

Esa ha sido mi presentación.

La señora **PARRA**, doña Andrea (Presidenta).- A continuación, tiene la palabra el señor Pablo Viollier.

El señor **VIOLLIER**.- Señora Presidenta, mi nombre es Pablo Viollier, soy analista de Políticas Públicas de ONG Derechos Digitales, una organización no gubernamental dedicada a la defensa, promoción y desarrollo de los derechos fundamentales en el entorno digital.

Nos dedicamos a todo lo relacionado con libertad de expresión, privacidad y acceso al conocimiento y, en general, a todo lo relacionado con derechos humanos y tecnología. Por lo tanto, nuestro giro está directamente relacionado con la materia que ustedes están investigando.

De hecho, nuestra organización redactó, en septiembre, un informe técnico-jurídico para la defensoría en el caso de

Operación Huracán, el que fue utilizado en el proceso y hoy se encuentra disponible en nuestra página *web.* En este informe se indican los defectos técnicos de esta supuesta interceptación y sus los problemas jurídicos, los que voy a pasar a exponer.

Mi presentación no tiene como objetivo establecer responsables concretos. En el caso en particular han intervenido –valga la redundancia- varios personajes bastante particulares, cuya responsabilidad no me parece realmente importante -eso lo está viendo la justicia en estos momentos-,pero sí me parece importante que se establezcan las responsabilidades institucionales del caso. No creo que este personaje tenga que ser utilizado como un fusible respecto de la responsabilidad institucional que corresponde en esta situación gravísima y que esta Comisión, en el fondo, aconseje los cambios regulatorios, legislativos y también disciplinarios, que permitan que esta situación gravísima y lesiva de los derechos fundamentales de las personas involucradas no vuelva a suceder. Por lo tanto, se complementa mucho con la presentación que hizo Paulo Colomés, que la hizo desde el lado técnico, pues yo no me voy a enfocar en si esto fue posible, en si se hizo o no, toda vez que esa es una teleserie que ya pasó y la están viendo en tribunales, pero sí me interesa abordar la parte jurídica.

Me parece que lo más grave fue que Carabineros tuvo la posibilidad de escapar a la regulación del Código Procesal Penal, vulnerando un principio fundamental de la reforma procesal penal, denominado el principio de no deliberación. Lo que establece este principio es que Carabineros de Chile es un auxiliar de la administración de justicia y no un interviniente al interior del proceso penal. Es decir, Carabineros realiza diligencias en función de la guía, dirección y fiscalización del Ministerio Público. En el fondo, es este ministerio el que tiene la facultad exclusiva y excluyente de la persecución penal y, en función de esta facultad, este ministerio ordena a Carabineros de Chile la realización de ciertas diligencias, pero Carabineros de Chile no se manda solo. Sin embargo, en este caso particular, la utilización de la Ley de Inteligencia permitió a Carabineros vulnerar este principio y mandarse solos, y operar al margen de la fiscalización y la guía del Ministerio Público, lo cual es sumamente grave, porque es una situación irregular, que vulnera el debido proceso de los inculpados y no le hace bien a la democracia, porque significa que Carabineros puede realizar diligencias por cuenta propia y, en el fondo, pasar a llevar el debido proceso y manchar, como vimos en este caso, casos específicos y vulnerar el derecho de las personas.

Creo que esto, en particular, sucede porque cada rama de las Fuerzas Armadas tiene una dirección de Inteligencia, las cuales pueden, a través de un procedimiento especial en la Ley de Inteligencia, realizar ciertas diligencias cuando están haciendo una actividad de inteligencia. Pero aquí hay que tener en consideración que hay dos ramas del derecho completamente distintas.

Una cosa es la inteligencia, la cual es una actividad de recopilación y de análisis de información para el efecto de

la toma de decisiones. Entonces, por ejemplo, hay organismos de inteligencia, como la ANI o la Dirección de Carabineros, que están investigando a los grupos eventualmente terroristas o subversivos y lo que hacen es recopilar información, analizarla y, basado en ello, se toman decisiones. En el fondo, se entrega información al Presidente de la República para que él pueda tomar ciertas decisiones. Este es un ámbito, el cual quedó muy claro durante la tramitación de la Ley de Inteligencia con algo que se llamó el principio de utilización exclusiva, es decir, que esta información es para efectos de inteligencia.

Otra cosa completamente distinta es el proceso penal, es decir, la investigación criminal, porque esta funciona a través del Ministerio Público, con la autorización del juez de garantía, cuando se realizan ciertas diligencias intrusivas, y al interior del proceso penal, regulado por el Código Procesal Penal, código que tiene sus propias formas y mecanismos de producción de pruebas. Por lo tanto, para pinchar un teléfono celular debo recurrir al artículo 222 del Código Procesal Penal, que establece la exigencia de una autorización previa del juez de garantía, por un período no máximo a 30 días, etcétera.

Entonces, aquí estamos en una situación sumamente irregular, dado que se genera un informe de inteligencia, a través de la Ley de Inteligencia, que permite un nivel de intrusividad mucho mayor que el Código Procesal Penal y que, luego, esa información se introduce dentro del procedimiento penal y se utiliza como prueba. Pero ahí hay varios problemas, porque, en realidad, se está utilizando una prueba producida a través de la Ley de Inteligencia al interior del proceso penal, prueba que fue producida con reglas completamente distintas. Entonces, por ejemplo, en la Ley de Inteligencia los estándares son mucho menores al momento de fundamentar la petición para realizar estas medidas intrusivas de la privacidad de las personas y de la inviolabilidad de sus comunicaciones, que son derechos constitucionalmente consagrados.

Por otro lado, la utilización no es dada por el juez de garantía, sino que es dada por un ministro de la Corte de Apelaciones del asiento de la jurisdicción. Además, los objetivos buscados son completamente distintos. En un caso, se busca y se recopila información para su análisis y generar datos de inteligencia y, en el otro caso, se busca evidencia para inculpar a una persona al interior del procedimiento penal.

Como les decía, en un caso, en la Ley de Inteligencia las policías pueden realizar esto en función de sus actividades de inteligencia, pero en el caso del proceso penal tiene que ser bajo la subordinación del Ministerio Público y esto no está sucediendo. Y la mejor forma de graficar, porque esta es una situación altamente irregular, es el hecho de que la fiscalía –recordemos- tuvo que pedir un peritaje de las pruebas que ella misma había presentado al interior del proceso penal. Uno se pregunta ¿cómo es posible que fiscalía tenga que pedir un peritaje de las pruebas que ella misma presentó? Y la razón por la cual tuvo que pedir peritaje de una prueba

que supuestamente es suya, fue porque esa fue prueba que fue producida en otra sede, en la sede de inteligencia, por Carabineros, y la fiscalía no tenía idea cómo se había producido esa prueba, bajo qué estándares, qué se había hecho. Simplemente llegó un informe de inteligencia, fiscalía asumió que todo estaba ahí en orden y lo presentó, pero ello es altamente irregular.

Entonces, en esa situación estamos ante una vulneración del debido proceso de los inculpados y una vulneración de su derecho a la privacidad y a la inviolabilidad de las comunicaciones, lo que me parece muy grave en términos jurídicos como democráticos, pues, en el fondo, esto permite a la policía decir: Bueno, no quiero pasar por todos estos enredos o todas estas garantías del proceso penal, entonces, lo hago a través de la Ley de inteligencia y después lo presentó como prueba y ello es muy grave y fue esto lo que (habilitó) toda esta situación.

La señora **PARRA**, doña Andrea (Presidenta).- Una consulta solo para entender, ya que uno es más lego en esta materia.

Cuando el uso de la información es para uno uso penal dentro de un proceso ¿tiene que autorizarlo el Ministerio Público?

El señor **VIOLLIER**.- El juez de garantía. La fiscalía solicita realizar una diligencia y el juez de garantía la autoriza.

La señora **PARRA**, doña Andrea (Presidenta).- Pero cuando el uso es respecto de información, ¿también tiene que ser autorizado?

El señor **VOILLIER**.- ¿Al interior del proceso penal?

La señora **PARRA**, doña Andrea (Presidenta).- No, no en un proceso penal, sino por la Ley de Inteligencia.

El señor **VOILLIER**.- Es que la Ley de Inteligencia es mucho más laxa, pues esta supone que usted es una agencia de inteligencia y que está buscando información y le dice que cuando usted busque información a través de medidas altamente intrusivas, entonces, vaya a pedir autorización a la Corte de Apelaciones.

La señora **PARRA**, doña Andrea (Presidenta).- Pero en un proceso penal no le pido al señor de la Corte de Apelaciones, sino que a un juez de garantía.

El señor **VOILLIER**.- Así es.

La señora **PARRA**, doña Andrea (Presidenta).- Entonces, aquí se mezclaron las dos cosas.

El señor **VOILLIER**.- Ese es el problema.

La señora **PARRA**, doña Andrea (Presidenta).- Tiene la palabra la diputada Maite Orsini.

La señorita **ORSINI** (doña Maite).- Señora Presidenta, un poco para entender. En este caso en particular, ¿quién solicita al juez de la corte esta autorización para intervenir el teléfono?

El señor **VIOLLIER**.- La Dirección de Inteligencia de Carabineros de Chile

La señorita **ORSINI** (doña Maite).- ¿Va Carabineros a la Corte y pide, haciendo uso de la Ley de Inteligencia, que se puedan intervenir los teléfonos?

El señor **VIOLLIER**.- Exactamente.

La señora **PARRA**, doña Andrea (Presidenta).- Es el juez de garantía quien le dice a Carabineros que está investigando tal caso que intervengan los teléfonos.

El señor **VIOLLIER**.- Ahora estamos ante un problema procesal, porque Carabineros de Chile está con una pata en Inteligencia y con la otra en la persecución penal, y a su vez, utilizando pruebas generadas en una sede, bajo ciertas reglas y, en otra, con otras reglas.

Pero también hay un problema fáctico, pues la ley de inteligencia permite la realización de diligencias mucho más intrusivas. El Código Procesal Penal solo permite la interceptación de comunicaciones, es decir, va una comunicación viajando, la intercepto y la analizo. Ese es el pinchado de teléfono, que es lo que se complica con el caso de las comunicaciones cifradas, porque se puede captar pero no descifrar.

Sin embargo, la ley de inteligencia permite diligencias mucho más intrusivas; no solo la captación, sino la intervención de sistemas informáticos. Ese tipo de intervención es bastante más lesivo, porque se puede ir a un sistema informático e intervenirlo. Además, es mucho más intrusivo, y se relaciona con un punto al que quiero pasar a continuación, cuando me refiera a la ilegalidad de la prueba.

Antes, decir que nos topamos con otro problema cuando hicimos este informe que redactamos a la Defensoría, que el control jurisdiccional que realizó la Corte de Apelaciones de Temuco fue altamente deficiente. Existe un principio de necesidad, es decir, estas pruebas deben realizarse cuando sea completamente indispensable, pero también existe un principio de especificidad, el cual tampoco se cumplió. No puedo ir a la corte de apelaciones, como agencia de inteligencia, a pedir un cheque en blanco y decir que quiero realizar diligencias de intervención de sistemas informáticos. Sin embargo, la corte aceptó que ellos realizaran diligencias de intervención de sistemas informáticos.

La ley de inteligencia es clara en cuanto al principio de especificidad, que responde a las siguientes preguntas:

¿Qué es lo que va a hacer usted, respecto de qué personas, por qué razón y cuál es la fundamentación?

Lo que vemos de la resolución de la Corte de Apelaciones de Temuco -no sabemos si es algo que se replica en el resto de las jurisdicciones- es que la corte simplemente está haciendo, en un proceso que además es secreto, un análisis completamente formal. ¿Es usted una agencia de inteligencia? Sí. ¿Me está diciendo qué es lo que va a ser, en términos más o menos amplios? Sí. Entonces, vaya y hágalo.

En consecuencia, no se está cumpliendo el principio de que exista un control respecto de las actividades que están realizando las agencias de inteligencia, lo que a nosotros nos parece sumamente grave.

La señora **PARRA**, doña Andrea (Presidenta).- Tiene la palabra la diputada Orsini.

La señora **ORSINI** (doña Maite).- Antes de pasar a la parte de la prueba, quiero detenerme en el tema de la autorización judicial.

Como usted bien dice que el estándar para obtener la intervención de un teléfono vía legislación común es muchísimo más alto –tiene que ser una pena de crimen, tiene que haber pruebas concretas-; el estándar es mucho más alto para que un juez de garantía autorice esta intervención usando la ley de inteligencia, en donde el estándar es menos exigente.

Entonces, el sentido común me dice que el cálculo que hace Carabineros es pensar que esta vía es más sencilla para acceder a estas intervenciones telefónicas, y lo hace a través de la corte de apelaciones. Sin embargo, me imagino que igual debe haber una fundamentación ante el juez de garantía para obtener la autorización de intervenir los teléfonos, y cuando se fundamenta debió haberse dicho que era para esta intervención penal.

Entonces, ¿no debió el juez de esa corte haber notado que no se podía hacer uso de esta ley para investigar penalmente y haber rechazado esta solicitud? A lo que quiero ir es a lo siguiente: ¿hay una responsabilidad del juez a la hora de dar la orden judicial, además de la de Carabineros?

La señora **PARRA**, doña Andrea (Presidenta).- Tiene la palabra el diputado Mellado.

El señor **MELLADO**.- Señora Presidenta, aprovecho de colgarme de la pregunta de la diputada para consultar si la ley de inteligencia le otorga al juez de la corte de apelaciones la facultad para controlar, o tiene el deber de controlar, lo que hagan quienes solicitan la interceptación telefónica. ¿Tiene la facultad para controlar o solo para otorgar la autorización, sin que posteriormente controle lo que se va a hacer?

La señora **PARRA**, doña Andrea (Presidenta).- Tiene la palabra el diputado Gutiérrez.

El señor **GUTIÉRREZ**.- Señora Presidenta, respecto de la discusión sobre los estándares, el estándar de la ley de inteligencia es menor, porque el objetivo que procura es reunir antecedentes para una toma de decisión política. Por eso el estándar es menor, no es casualidad, y no tiene como objetivo que sea medio de prueba para configurar algún tipo de responsabilidad penal y llevársela a un juez. Son estándares distintos, y es razonable lo que se da en la mencionada ley.

Lo que sucede es que el Ministerio Público solicitó este peritaje para saber si la prueba que había presentado Carabineros era verdadera, porque se dieron cuenta de que este sistema operativo, Antorcha, era falso.

La pregunta que cabe hacerse es qué hubiera pasado si ellos no se hubiesen dado cuenta de que esta prueba que había entregado Carabineros a través de este sistema Antorcha era falsa. Lo más probable es que ellos hubieran perseverado en la imputación de responsabilidad penal, a través de los antecedentes que le había entregado Carabineros, que era una información obtenida por la ley de inteligencia y no a través de los cauces del Código Procesal Penal. Por lo tanto, la prueba estaba viciada.

La Fiscalía cuestionó la prueba rendida por Carabineros, porque lo que le había entregado era falso, no porque lo hubieran conseguido de manera irregular, al "engañar" a un ministro de corte, al hacerse todas las pericias a través de la ley de inteligencia. Ello, porque el señor Smith sostiene -no sé si será creíble ahora- que cuando estaban grabando o interceptando los teléfonos, había fiscales presentes; es decir, mientras Carabineros estaba reuniendo la información a través de la ley de inteligencia estaban los fiscales presentes. Por tanto, eso es mucho más grave aún, porque los fiscales sabían que Carabineros estaba obteniendo la información a través del uso de esta ley y no por el Ministerio Público, pidiéndole a los jueces que fuesen al juzgado de garantía a pedir la autorización para la interceptación.

Entonces, todos estaban actuando de manera ilegal, porque sabían que estaban reuniendo información de manera indebida. Pero todo esto se viene abajo por el mecanismo que estaban utilizando para reunir antecedentes, que era el sistema operativo Antorcha, que en realidad era un engaño de Smith.

Sin embargo, todo esto se resume en que alguien les impuso una prioridad a las policías y al Ministerio Público de que debían reunir antecedentes. Como debían reunir antecedentes, todos se pasaron la legalidad por "buena parte", porque los necesitaban para juzgar y condenar a los mapuches involucrados en tal o cual delito.

Por tanto, hay una responsabilidad, como nuestro invitado bien señaló, que no puede ser cortada en un fusible como Smith, sino que alguien tiene que haber tomado la decisión. Insisto, los fiscales estaban al lado de los carabineros que estaban pinchando los teléfonos, sabiendo que habían obtenido la orden de un ministro de corte y no de un juez de garantía.

Entonces, mi pregunta es si es posible pasar por alto o superar un Estado de derecho, con tal de conseguir las pruebas necesarias para inculpar a alguien.

La señora **PARRA**, doña Andrea (Presidenta).- Les recuerdo que tenemos conocimiento de que esta orden de interceptar teléfonos del juez de la Corte de Apelaciones, señor Padilla, fue dictada en forma retroactiva, lo que es altamente irregular.

Tiene la palabra la diputada Nuyado.

La señora **NUYADO** (doña Emilia).- Me parece bien la acotación que usted hace cuando señala que se deben establecer responsabilidades institucionales, por lo que me gustaría tomar esa sugerencia para que esta comisión pueda incorporarla posteriormente en las conclusiones.

También me interesa saber cuál sería aquella sugerencia sobre el control jurisdiccional que debiera haber tenido la Corte de Apelaciones de Temuco y que, sin embargo, no cumplió, y lo que ha planteado y se ha visto ha sido una situación ineficiente y grave. ¿Cuáles serían esas sugerencias?

La señora **PARRA**, doña Andrea (Presidenta).- Tiene la palabra el señor Viollier.

El señor **VIOLLIER**.- Señora Presidenta, respecto de la pregunta de la diputada Orsini creo que hay un principio de uso exclusivo de la información. Lamentablemente ese principio se discutió y hubo un consenso en la tramitación. Si se lee la historia de la ley hay un consenso en que el uso de la información que se recabe al interior de la actividad de inteligencia, en el Sistema Nacional de Inteligencia, iba a ser para uso exclusivo de inteligencia que, como bien dice el diputado Gutiérrez, es un uso más bien político.

Sin embargo, esos principios no se ven bien reflejados en el texto de la ley. De hecho, el texto de la ley da a entender que esta información puede ser incluso dejada bajo ciertas circunstancias o bajo ciertos procedimientos, donde tiene que concurrir el ministro del Interior, el subsecretario, e incluso pueden ser liberados procesos y requisitos que por lo demás no se cumplieron en este caso. O sea, en ningún momento el subsecretario de la época, el subsecretario Aleuy, fue y firmó este asunto.

Eso es lo que da pie a este uso. De hecho, el diputado Gutiérrez tiene razón. El análisis y la recolección de información es para la toma de decisiones, es decir, yo como Estado tengo organismos de inteligencia y esos han detectado células terroristas en tal lugar y, por tanto, los vamos a investigar con más cuidado y vamos a mandar un agente encubierto y vamos a tomar decisiones respecto de eso, pero después usted verá cómo genera pruebas para meter a esa persona en la cárcel. Vaya usted, Carabineros de Chile, ponga un agente encubierto, de acuerdo con el Código Procesal Penal, junte la evidencia y haga la persecución penal, pero es efectivamente para la toma de decisiones.

Lamentablemente, en este caso no ha sido así y ha sido utilizado al interior del procedimiento penal. Yo creo que aquí una institución que ha salvado y ha salido libre de polvo y paja es fiscalía. O sea, esta situación no es nueva.

No es nuevo que se utilicen estos informes de inteligencia al interior del procedimiento penal. Recordemos que en el caso de Bombas parte de la información que se cayó por pruebas ilícitas dentro de la investigación eran informes de inteligencia y hay un principio en el Derecho Procesal Penal que es el del árbol envenenado. Ese principio dice que si una prueba fue utilizada, fue producida de forma ilícita, no puede ser utilizada y no tiene que ser tenida en consideración al momento de verificar si una persona es culpable o inocente. De hecho, hay todo un procedimiento al interior del proceso penal de exclusión de prueba por pruebas ilícitas. En el caso Bombas se excluyeron esos informes de inteligencia porque decían que esa prueba no podía ser tenida en consideración porque no fue producida de acuerdo con las reglas del código que nos rige, sino que por otras reglas. Sin embargo, no me sorprendería –yo no tengo datos- que muchas personas hasta hoy hayan sido condenadas utilizando este subterfugio.

Si nosotros pensamos, la única razón por la cual la fiscalía puso el grito en el cielo fue porque Carabineros de Chile estaba espiando a la abogada asistente de un fiscal y recién cuando empezaron a espiar a la abogada asistente de un fiscal dijeron: Resulta que esta cuestión parece que es falsa. Entonces, vamos a pedir un peritaje respecto de la prueba que nosotros mismos presentamos, pero fiscalía en el pasado nunca ha tenido problemas para ingresar informes de inteligencia como prueba penal. De hecho, es bastante cómodo para fiscalía y fue recién cuando surgió esta disputa institucional entre la fiscalía y Carabineros, porque fiscalía no se quería hacer cargo del bochorno institucional que significaba tener este supuesto *software*, que es completamente vergonzoso que no es cierto y que es falso y Fiscalía no quería verse involucrada en este proceso en donde se viese que hay pruebas derechamente falsas presentadas por su parte que pidió este peritaje, pero en el pasado se ha utilizado esto siempre.

Respecto del rol que tiene la corte al momento de controlar –usted me decía que había un control *ex post* o solamente una autorización- la inteligencia, la ley de inteligencia habla de una autorización. Sí establece criterios que creemos que no se cumplieron en este caso en específico. Tenemos la sospecha fundada de que no se está cumpliendo en general, es decir, que es un principio de que la información o la diligencia tiene que ser completamente indispensable, con un criterio de necesidad, pero también un criterio de especificidad. La corte no puede autorizar la realización de diligencias de cheque en blanco. O sea, yo voy a intervenir sistemas informáticos, pero, ¿cuáles sistemas informáticos se van a intervenir? ¿Por qué los va a intervenir? ¿A través de qué medios los va a intervenir? ¿Por cuánto tiempo?

Respondiendo a otra pregunta que hizo el mismo diputado respecto de estas listas de teléfono, nosotros tuvimos una mesa redonda de discusión de este tema porque estuvimos muy metidos, invitamos a la fiscalía, invitamos a académicos, invitamos a la defensoría y la defensoría decía que estas listas de la PDI son completamente poco profesionales. Se trata de un Excel en donde tú dices: Bueno, tal persona.

¿Cuáles son los números asociados a tal persona? 9 números. Y esos números, ¿qué criterios de asociatividad cumplen? ¿En qué sentido están asociados a esa persona? ¿Es su número personal? ¿Es el número de un familiar? ¿Es el número de su trabajo? No, simplemente la PDI presenta una lista de números asociados y resulta que en el caso de la Operación Huracán había una persona con 8 números asociados y eran el número de la mamá, del amigo, del hermano y ninguno de esos 8 números era su número personal. Entonces, la falta de profesionalismo y el hecho de que las cortes de apelaciones permitan ese nivel de arbitrariedad y de poca especificidad nos parece que es sumamente preocupante.

Respecto de los controles y de la responsabilidad institucional es justamente lo que corresponde a mi última parte de la intervención y por eso lo pospondré un poco.

Pasando al siguiente punto, ya hablamos de que esta prueba fue generada en sede de inteligencia y que al interior del proceso penal es ilegal. Si se analiza esta situación, resulta que esa prueba era aparentemente falsa. Yo dejé de seguir la teleserie en algún momento, pero entiendo que hubo un peritaje de la PDI o de otro organismos de 200 páginas que demostró que esos mensajes eran completamente falsos, pero si la aseveración de Carabineros fuese verdadera resulta que esa prueba o lo que se realizó es incluso ilegal al interior del proceso de inteligencia, que ya vimos que es particularmente permisivo y amplio.

En derechos digitales nos agarrábamos la cabeza porque en septiembre, cuando salió esto a la luz, se suponía que esta era una intervención de comunicaciones. Dijimos que esto era completamente imposible porque se pueden intervenir las ondas que viajan, pero esa información, como bien explicó Paulo, está cifrada y la persona que logre descifrar el cifrado se va a hacer millonaria y sería una noticia a nivel mundial. Entonces, esa información tiene una clave, está encriptada, está cifrada. Se puede interferir esa información, pero son puros garabatos. ¿Cómo se podría pasar eso? Dudo que Carabineros de Chile tenga al mejor experto en cifrado del mundo.

Después resulta que esto era un *keylogger*, eso significa que a uno lo infectan con un programa malicioso que es capaz de tener un registro de lo que se teclea en el teléfono. Nosotros dijimos, perfecto, puede ser un *keylogger*, pero un *keylogger* solo da la mitad de la conversación, la mitad de lo que la persona está tecleando. ¿Cómo fueron capaces de reconstruir esas conversaciones? Tendrían que haber infectado a las dos partes de las conversaciones y ver que uno estaba conversando con el otro. Es muy difícil.

Después, resulta que esto era un espejo, entonces había un asunto de espejo en donde podían replicarlo y nosotros decíamos que entonces habría que pedir al ISP, a la empresa de telecomunicaciones, que clonara la SIM, pero creo que las empresas de teléfonos no se prestarían para eso.

Finalmente, esto era un *malware*, o sea, un programa malicioso. Quiero ser muy enfático al decir que para hacer eso y como Alex Smith supuestamente trató de presentarlo en el programa de televisión –imagino que también lo vino a pre-

sentar acá- significa algo que es sumamente grave en términos de estado de derecho. Significa que Carabineros de Chile pretende echar mano a las herramientas de los delincuentes informáticos para efectos de recolección de pruebas y eso es muy grave porque si ustedes vieron el programa con Sutherland, y que mostró Paulo, en el fondo lo que hacía era decirle: nosotros les mandamos unos mails falsos diciendo que esta era una promoción, etcétera, y con eso obteníamos su clave y su usuario y con eso yo puedo acceder a su correo.

Hay un término para esa actividad y se llama *phishing,* es un delito y es castigable por nuestra ley de delitos informáticos y no es posible que nuestras policías echen mano a las herramientas de los delincuentes informáticos para recolección de pruebas y es ilegal de acuerdo con el Código Procesal Penal porque este solo permite la interceptación de comunicaciones, pidiéndoselo al ISP con una orden judicial previa, etcétera, pero también es ilegal de acuerdo con la ley de inteligencia porque esta ley permite intervenir un sistema informático. Es decir, yo tengo las herramientas de un sistema informático, accedo a él de forma informática, pero aquí estamos ante un uso fraudulento, de un engaño. Es decir, que Carabineros de Chile diga que es una empresa y que está mandando una promoción para que el destinatario haga clic en un archivo que remite a un formulario donde se debe poner el nombre del usuario y la contraseña. A través de eso Carabineros pretendía que era legítimo instalar un programa malicioso en el celular del imputado.

Quiero ser enfático en lo peligroso que es esto. Me gustaría desmarcarme de la tónica que se ha dado hasta el momento, que se refiere a que no hay escándalo, que era falso, que no funcionaba. Yo digo todo lo contario. Por suerte que no funcionaba, porque si hubiese funcionado estaríamos ante una vulneración muy grave de los derechos fundamentales de las personas.

Pongo un ejemplo. El gobierno mexicano contrató la empresa italiana Hacking Team y adquirió el *software* Pegasus, que funcionaba de la misma manera. Me imagino que la agencia de inteligencia o la policía, que no se caracteriza por ser muy legítima en México, enviaba mensajes de texto no solo a personas del crimen organizado, sino que también a periodistas, a opositores políticos, a defensores de los derechos humanos. Dicho *software* no solo permitía acceder al WhatsApp, sino además a la cámara, a la geolocalización, al micrófono, a todo lo que se podía teclear. Es decir, permite un control absoluto de la intimidad total de una persona.

Personalmente, mis cosas íntimas pasan dentro del celular o cerca, porque ando con mi celular para todas partes. Entonces, todo lo que hablo pasa cerca del celular y todos mis archivos, *mails* y contactos están en el celular.

Por lo tanto, la idea de que Carabineros de Chile utilice una medida intrusiva a través de un engaño como instalar un *software* espía, que es completamente ilegal, es muy grave.

Hoy no estamos tan lejanos de esa situación, porque cuando se conoció el escándalo de Hacking Team, en 2016, hubo una revelación a nivel mundial porque dicha empresa fue

“hackeada” y se subió el código fuente de su programa, pero también se subió un *terabyte* de información con todos los correos electrónicos, y había correos entre la Policía de Investigaciones y Hacking Team; había correos donde un representante de la Policía de Investigaciones decía explícitamente que ellos querían adquirir el *software* para obtener información a la que no podían acceder sin una orden judicial.

Nosotros hicimos ruido, etcétera, y la Policía de Investigaciones emitió una declaración pública señalando que no habían adquirido nada, pero después emiten otra aclarando que habían adquirido el *software*, pero solo para uso legítimo.

A nosotros nos aterra la posibilidad de que Carabineros de Chile pueda estar utilizando este tipo de herramientas, y por eso estamos felices de que en este caso la herramienta haya sido falsa y no esté siendo utilizada.

Señora Presidenta, quiero ser enfático en que el uso de ese tipo de herramientas es ilegal de acuerdo con el Código Procesal Penal y la Ley de Inteligencia.

Volviendo a las responsabilidades institucionales, me parecen sumamente graves las declaraciones del general Blu, quien se lamentó públicamente. Hubo cosas muy irregulares, como que Carabineros se haya opuesto físicamente a la realización de la incautación. Eso es muy grave en un Estado de derecho.

El general Blu, en el ejercicio de sus funciones, en una entrevista lamentaba que esto saliera a la luz, porque dijo expresamente que de ahora en adelante los delincuentes informáticos van a saber que no tienen que hacer clic en los enlaces sospechosos porque como ya se sabía no podrían seguir utilizando esa herramienta. Eso quiere decir que al menos en la Dirección de Inteligencia de Carabineros, pero me imagino que también en otras agencias de inteligencia, existe el ánimo de seguir utilizando este tipo de herramientas. Como dije, esto es muy grave y vulnera los derechos de las personas.

No puede ser que la Presidenta Bachelet en marzo de 2017 haya lanzado una política nacional de ciberseguridad en donde este tipo de herramientas se declaró completamente ilegal, declarando octubre como el mes nacional de la ciberseguridad, estableciendo medidas para educar a las personas para que no hagan clic en los *link* maliciosos, que no caigan en *fishing*, se ratifica el Convenio de Budapest, se modifica la ley de delitos informáticos, se tipifica el *fishing* para perseguir la actitud delictiva, pero resulta que nuestras policías no solo la están utilizando, sino que se lamentan públicamente de que esto salga a la luz porque quieren seguir utilizando esta herramienta en el futuro.

Eso es gravísimo, porque da luces de que quieren seguir utilizando esa herramienta. Me parece que el Estado no puede borrar con el codo lo que se escribió con la mano. Por lo tanto, no puede lanzar una política nacional de ciberseguridad y, por el otro, que sus policías estén ejecutando ese tipo de actividades.

Por otro lado, al interior del proceso mismo –volviendo al tema del debido proceso-, aquí hubo algo muy grave: la total falta de transparencia respecto de cómo se obtuvieron

las pruebas. Sabemos que las pruebas se consiguieron de forma ilegal, en el sentido de que se utilizó prueba generada en el proceso de inteligencia al interior del proceso penal, y luego a los imputados se les dijo que tenían todas sus conversaciones. Se les pasó las conversaciones transcritas en un papel, pero está el principio de igualdad de armas. Es decir, si una parte tiene una prueba que inculpa a otra, esta debe tener la capacidad de desvirtuar esa prueba, de decir que la prueba no es verdadera por uno, dos y tres. Pero si el imputado no sabe cómo se generó dicha prueba, ¿cómo va a tener la capacidad de desvirtuarla?

Por ejemplo, alguien puede decir que tiene todos los wathsapp de una persona y dicen tal cosa, pero el imputado puede decir que son falsos porque nunca los ha enviado. Pero si no se sabe cómo se generaron, bajo qué herramienta, bajo qué condiciones, ¿cómo se podrá desvirtuar es prueba? En el fondo, es una vulneración gigantesca al debido proceso porque no permite a los defensores contar con las herramientas para desvirtuar esa prueba. Eso es altamente irregular y complejo en término de los derechos de los imputados.

Por último, volviendo al tema más técnico, hubo completa falta de profesionalismo al interior de la cadena de custodia de la prueba digital. Entiendo que en el informe pericial está comprobado de que estos celulares, luego de ser incautados, fueron intervenidos y aparecieron archivos en formato ".txt" dentro de una carpeta que no correspondía en absoluto.

Si ustedes ven cualquier película de detectives, cuando llegan los forenses a una escena del crimen nadie entra, sacan fotos, guardan esas fotos, mantienen un registro, porque debe haber una custodia de la evidencia. Se procede de esa forma para que nadie llegue a la escena del crimen e implante un cuchillo. Eso también corre para la evidencia digital.

Sin embargo, resulta que en todas y cada unas de las etapas de la supuesta custodia de esta evidencia digital no hubo ningún tipo de resguardo. Se conectaron los terminales a internet luego de haber sido incautados los equipos y se metieron dentro de los terminales archivos foráneos, los que además estaban en formatos completamente editables. Los correos supuestamente interceptados los operaba el personaje que prefiero no nombrar, y el general Blu, en sus correos electrónicos personales y se los reenviaban.

Por lo tanto, en todas y en cada una de las etapas de la custodia digital no se respetaron los estándares y, además, se realizaban en archivos completamente editables.

Entonces, ¿qué derecho de defensa tiene un imputado si la evidencia digital que se produjo en su contra en el proceso de investigación pudo haber sido editada por cualquiera de las personas que lo perseguía?

El señor **COLOMÉS.**- Señora Presidenta, quiero hacer un alcance al respecto aprovechando el tema de la custodia de evidencia digital.

En algún momento se mencionó que el problema con estos teléfonos era que no se habían puesto en modo avión y por

eso, en teoría, la aplicación espía seguía conectada y generando información.

Lo que recomendaba Carabineros fue haber puesto en modo avión el teléfono antes de incautarlo, pero resulta que eso atenta completamente contra los principios de recolección de evidencia digital que dicen justamente lo opuesto: cuando hay que periciar un dispositivo electrónico ni siquiera se puede apagar porque la memoria del equipo todavía tiene datos que pueden ser extraídos.

Hay una contraposición bastante llamativa y se ha evidenciado que la cadena de custodia nunca se respetó.

La señora **PARRA**, doña Andrea (Presidenta).- Tiene la palabra, señor Viollier.

El señor **VIOLLIER**.- Entonces, volviendo a la pregunta de la diputada, mi intervención tiene como objetivo, no establecer responsabilidades individuales ni que la responsabilidad se corte por el hilo más delgado. Será función de la justicia que estas personas enfrenten sus responsabilidades. Sin embargo, creo importante que la comisión analice la posibilidad de establecer responsabilidades institucionales y la recomendación de modificación regulatoria legislativa, en el fondo, del *modus operandi* de nuestras fuerzas policiales, de forma tal que una situación vulneratoria de derechos fundamentales y de derechos humanos como la acaecida, también con la correlativa mancha al prestigio de un sinnúmero de nuestras instituciones, no vuelva a ocurrir.

En ese sentido, el primer paso es que esta comisión recomiende la modificación de la "ley de Inteligencia", de forma tal que la consagración del principio de uso exclusivo de información recopilada, no solamente conste en la historia de la ley, sino que también se establezcan criterios claros respecto de las circunstancias en que un informe de inteligencia puede ser utilizado en el procedimiento penal.

La interpretación de la organización que represento es que tiene que haber una separación total entre ambas disciplinas. Hay países que optan por esa modalidad y otros por establecer un procedimiento muy reglado respecto de las circunstancias específicas y excepcionales en que puede utilizarse información de inteligencia en un procedimiento penal. Les recomendaría una separación tajante, porque la recopilación de información responde a objetivos distintos, bajo condiciones distintas.

Siguiendo el espíritu de la política nacional de ciberseguridad, que se establezca una prohibición a la utilización de herramientas excesivamente intrusivas, como la utilización de *malware,* de códigos maliciosos a través de *phishing* por parte del Estado. No se puede vivir en un Estado de derecho en donde el Estado pretenda engañar a sus ciudadanos para instalar códigos o *software* maliciosos que sean capaces de controlar completamente nuestros celulares. Debe mantenerse un balance entre el poder público y su capacidad de injerencia en nuestras vidas privadas. No se puede afectar el Estado de derecho.

Por lo tanto, recomendamos a la comisión estudiar una modificación legislativa que prohíba este tipo de herramientas excesivamente intrusivas.

También, una modificación a la "ley de Inteligencia" que establezca un mayor nivel de control por parte de las Cortes al momento de autorizar este tipo de diligencias provenientes de este procedimiento especial de inteligencia, de manera que el control que hagan las Cortes no sea puramente formal, sino material y sustantivo de la actividad de inteligencia, siguiendo criterios de un Estado de derecho.

Por último, la modificación de estándares institucionales al interior de Carabineros de Chile y del resto de las instituciones dedicadas a la persecución penal y también a la actividad de inteligencia respecto de establecer criterios técnicos estrictos en relación con la cadena de custodia de evidencia digital. Esto es algo que no solamente va a operar para casos de terrorismo. Hoy, prácticamente todos y cada uno de los delitos tiene un componente informático, no por su comisión, sino por las medidas de prueba. En consecuencia, es insostenible que al año 2018 no existan criterios claros, profesionales y técnicos respecto de cómo se va almacenar la prueba digital, porque es algo de lo cual, durante el siglo XIX, nosotros nos hicimos cargo de que sí se respetaran, tanto las cartas como el resto de las pruebas que se utilizan en los procedimientos penales. Por lo tanto, es algo que se debe incorporar para consagrar tanto el derecho al debido proceso como la igualdad de armas de los imputados respecto de las evidencias que hoy se generan en un porcentaje gigantesco de investigaciones por drogas, pero también en hurtos y otros delitos, porque en algún sentido la coordinación, la evidencia pasa por *WhatsApp*, por los celulares, porque básicamente es la forma en que todos y cada uno de nosotros nos comunicamos en el día a día.

Entonces, junto con agradecer la invitación y la posibilidad que nos han dado para entregarles nuestros descargos como organización, quiero decir que estamos completamente llanos a ser convocados nuevamente para ofrecerles recomendaciones más precisas y aclarar cualquier duda que tengan respecto de la materia.

La señora **PARRA**, doña Andrea (Presidenta).- Antes de ofrecer la palabra a los diputados, voy a recabar el acuerdo para, primero, enviar un oficio a Carabineros de Chile, a fin de que informe cuál es la situación actual de los teléfonos de los generales en relación con el tema de los parches, porque, en verdad, estamos todos inquietos. La última información fue que estos parches permanecían en los teléfonos de los generales y, al parecer, nadie ha hecho nada. Entonces, lo lógico es oficiar para saber si eso se revisó, si fue periciado y si fueron eliminados de los teléfonos.

¿Habría acuerdo?

Acordado.

En segundo lugar, pido el acuerdo para enviar un oficio a Carabineros de Chile, para que nos informe respecto del test psicológico realizado a don Alex Smith, qué profesional

lo realizó y en qué fecha, más que el diagnóstico, porque es información reservada.

¿Habría acuerdo?

Acordado.

Tiene la palabra el diputado Miguel Mellado.

El señor **MELLADO**.- Señora Presidenta, Paulo Colomés dijo que había elaborado un informe en derecho y que lo había presentado en la causa. Sería bueno, para las conclusiones, tenerlo a la vista.

La señora **PARRA**, doña Andrea (Presidenta).- ¿Habría acuerdo para solicitar el informe?

Acordado.

Tiene la palabra el señor Pablo Viollier.

El señor **VIOLLIER**.- Señora Presidenta, no tenemos problemas para remitirle el informe. Sin embargo, nos demoramos en subirlo a la página por un tema de reserva judicial. Esos procesos están terminados, por lo cual preguntamos a la defensoría si la información podía ser pública. Hoy está en nuestra página web y la vamos a enviar a la secretaría de la comisión.

Solo quiero hacer la salvedad de que ese informe fue elaborado durante septiembre del año pasado, por tanto, la parte jurídica sigue siendo completamente atingente, porque es un análisis. En el fondo, todo lo que les he explicado respecto del principio de utilización exclusiva, de la autorización de la Corte de Apelaciones, de la historia de la "ley de inteligencia", de la separación entre inteligencia y persecución penal, en fin, está todo actualizado, porque no ha cambiado la legislación.

Sin embargo, el análisis técnico de las herramientas responde a la aseveración de Carabineros de que esto era una interceptación de comunicaciones. Entonces, el análisis está en función de subvertir la tesis de que era un *keylogger*, después, que era un espejo, después, que era un *phishing*, y después un *malware*.

Por lo tanto, el informe responde al estado del arte en ese momento, y no es algo que pueda ser utilizado hoy como análisis técnico. Solo para que quede constancia.

La señora **PARRA**, doña Andrea (Presidenta).- Tiene la palabra la diputada Emilia Nuyado.

La señora **NUYADO** (doña Emilia).- Señora Presidenta, ha quedado bastante claro, en las dos exposiciones, cuáles deberían haber sido los procedimientos, pero me hubiese gustado algunas de las recomendaciones con respecto a la fiscalía, porque como bien usted señaló en sus análisis que si no hubiese sido afectada una de sus funcionarias, o alguno de ellos, en verdad, no estaríamos en una situación como la "Operación Huracán" y tampoco en esta comisión. Íbamos a tener a nuestro *lamngen* preso, hasta el día de hoy, y ninguna de las defensas habría tenido las pruebas suficientes a disposición. Por lo tanto, a mí me preocupa eso, la actitud

que ha tenido la fiscalía, la actitud que ha tenido la Corte de Apelaciones de Temuco, e independientemente de las solicitudes e invitaciones que se hicieron, lamentamos no haber tenido a nadie en la comisión.

Entonces, no sé cuál debiera ser la recomendación, entendiendo que esta exposición es pública, que hay situaciones complejas que el gobierno debiera analizar respecto de lo que ocurrió, y yo esperaba alguna recomendación respecto de la fiscalía.

La señora **PARRA**, doña Andrea (Presidenta).- Tiene la palabra el diputado Hugo Gutiérrez.

El señor **GUTIÉRREZ**.- Señora Presidenta, don Pablo Viollier habló de la ley de inteligencia y del Código Procesal Penal, y dijo que sería mejor que no se pudiesen utilizar como prueba los antecedentes obtenidos mediante la ley de inteligencia, durante el juicio penal. Mi pregunta para el señor Viollier es si eso se puede hacer hoy. Es decir, quiero saber si existe algún mecanismo jurídico que permita la utilización de los antecedentes reunidos en virtud de la ley de inteligencia en el proceso penal como prueba de responsabilidad penal. ¿Por qué el señor Viollier es tan categórico al decir que mejor no, que esto de acá no puede ser pasado para allá?

Los estándares internacionales para las policías, para la cadena de custodia de la prueba digital, ¿dónde están establecidos? Es posible que alguien nos indique cuáles son, para conocerlos y tener claridad al momento de sugerir algún tipo de pauta u orientación en el informe.

La señora **PARRA**, doña Andrea (Presidenta).- Tiene la palabra el señor Pablo Viollier.

El señor **VIOLLIER**.- Señora Presidenta, por su intermedio, usted tiene la razón sobre que no me referí a la fiscalía en particular, específicamente porque goza de autonomía constitucional, pero, también, porque aquí hay un área gris. Y aprovecho de contestar la pregunta del diputado Gutiérrez. En las recomendaciones está que la comisión estudie la posibilidad de sugerir una modificación legislativa a la ley de inteligencia, porque en este campo hay un área gris respecto de hasta qué punto se pueden utilizar estos informes de inteligencia en el procedimiento penal. La admisibilidad de esa prueba va a depender del criterio del juez de garantía. Les adelanté que en el "caso bombas" esa prueba fue declarada ilegal, por la teoría del árbol envenenado. Reitero, hoy existe esa área gris.

No me atrevo a especular sobre el nivel de presión que tiene la fiscalía para efectos de lograr casos concretos en el sur de Chile. Mi criterio es que esta información no se puede utilizar en casos concretos. Fíjense que la ley de inteligencia establece que el tribunal puede solicitar a la Agencia Nacional de Inteligencia la entrega de esa información y exige la concurrencia de ciertos personeros, creo que del subsecretario o del ministro del Interior y otra autori-

dad, y en este caso eso no sucedió. La ley establece que el tribunal debe solicitar dicha información y, en este caso, el tribunal no la solicitó, sino que fue presentada como prueba por la fiscalía.

Otra hipótesis es que estos informes de inteligencia se liberen, es decir, se entreguen al dominio público y, estando en el dominio público, pueden ser presentados como prueba.

Otro subterfugio que se ha utilizado es la realización de peritajes a cargo de las mismas personas que hicieron el informe de inteligencia. En el fondo, ese peritaje es la lectura del informe de inteligencia y la prueba es el relato oral del informe de inteligencia.

Hay un área gris y, en la medida en que exista esa área gris, la fiscalía puede echar mano de esta técnica, de este subterfugio, que considero impropio, toda vez que vulnera el debido proceso de los imputados y el espíritu de la ley.

Usted me preguntaba en qué lugar concreto. Yo les dije que aquí no se cumplieron las hipótesis particulares; pero, además, les dije que el espíritu de la ley de inteligencia establece el principio del uso exclusivo y que lo que se debe hacer para que esta situación no se repita es modificar la ley para que quede totalmente claro, no solo en la historia fidedigna del establecimiento de la ley, que esta información es para efectos de inteligencia y no para otros efectos.

Respecto de los estándares internacionales de prueba digital, la verdad es que no soy parte de la comunidad técnica, pero sí existen. En Derechos Digitales tenemos un área técnica con dos ingenieros informáticos que trabajaron en el informe de la defensoría y que sí conocen este tipo de estándares. No sé si Paulo sabe un poco sobre esto, pero estos estándares de cautela al interior de la cadena de custodia de evidencia digital existen en otras latitudes, en otras jurisdicciones y es algo que puede tenerse en consideración al momento de exigirle a Carabineros… Esto es un poco de *accountability*, es decir, hasta qué punto hacemos que nuestras policías respondan a criterios de debido proceso, a la responsabilidad que se les presenta al momento de generar evidencia, y esto es algo que necesita un criterio de profesionalismo, pero también un criterio de responder ante la sociedad y ante los requisitos procesales establecidos en nuestra legislación.

La señora **PARRA**, doña Andrea (Presidenta).- Tiene la palabra el señor Paulo Colomés.

El señor **COLOMÉS**.- Señora Presidenta, hay una normativa internacional, la norma ISO 27001, de 2013, que menciona los temas que el diputado consultó. Si a usted le interesa, se puede hacer llegar a su correo electrónico o me puede solicitar a mi dirección de correo más información de lo que necesite.

La señora **PARRA**, doña Andrea (Presidenta).- Señor Colomés, se lo vamos a pedir.

También quiero recabar el acuerdo para oficiar a la Biblioteca, a fin de que elabore un informe sobre los están-

dares técnicos de cadena de custodia de evidencia digital que existe en otras legislaciones, de manera de utilizar dichos antecedentes como elementos para el trabajo de la comisión.

¿Habría acuerdo?

Acordado.

En la comisión también compartimos la preocupación por muchos de los aspectos que plantearon nuestros invitados.

Créannos que nos parece gravísimo lo que ocurrió con la oposición física de otra institución al allanamiento de la PDI. Eso nos habla de una institución con excesiva autonomía, que hoy se toma estas facultades. Y pareciera que este hecho no es un escándalo nacional, sino que más bien lo vimos como un hecho de la causa.

También nos llama mucho la atención el uso de herramientas como el *phishing* o las que nuestro invitado señaló como altamente intrusivas; la producción de pruebas y la falta de profesionalismo en la cadena de custodia.

Nos sigue llamando la atención que no se asuma una responsabilidad institucional frente a estos temas, el que ningún técnico de Carabineros advirtiera o al menos revisara qué se estaba haciendo en una situación tan grave como la que hoy se señaló. Nos preocupan cuántas personas más pudieron haber sido afectadas por una situación como esta, en términos irregulares.

Créanme que también nos preocupa mucho la situación de los fiscales, porque no está clara la participación de algunos de ellos, como el fiscal Arroyo, que también es parte del proceso investigativo, porque las versiones no cuadran: se dice que no contaba con información y pareciera que hay antecedentes distintos.

Nos preocupa que el actual jefe de la Dirección de Inteligencia, quien estuvo en la Comisión hace un par de semanas, nos dijera que no han hecho nada con los parches en los teléfonos, que ahí están y que nadie ha tomado decisión alguna. Nuevamente, eso nos habla de la precariedad en la institución de Carabineros.

En fin, la verdad es que estamos bastante preocupados.

Agradecemos mucho lo didáctico de ambas exposiciones. Aprovecho de pedirles, con mucha humildad, que nos permitan contar con sus opiniones profesionales, al menos vía correo electrónico o teléfono, sobre todo porque se aproxima la etapa de elaboración del informe y nos interesa mirar esto desde la perspectiva de las modificaciones que podamos introducir y las sugerencias que podamos plantear frente al caso.

Si hay alguna otra consulta u otro comentario final, ofrezco la palabra.

Tiene la palabra el señor Colomés.

El señor **COLOMÉS.**- Señora Presidenta, solo quisiera completar el tema de los parches de los celulares de los generales. Carabineros, desde ya, debiese solicitar un peritaje a los celulares –no lo había mencionado-, aplicarles la cadena de custodia que corresponde y determinar si efectivamente se instaló un *malware* espía o una solución homeopática, que realmente no hace nada contra un *software*. Se debe determinar a través de un proceso legítimo y válido, mediante una insti-

tución o empresa reconocida en el rubro; en Chile hay muy buenas en eso. Incluso, la misma PDI cuenta con especialistas bastante avanzados en materia forense. Por lo tanto, los recursos están, es cosa de solicitarlos.

El señor **GUTIÉRREZ**.- Señora Presidenta, en el mismo sentido de lo manifestado por el señor Colomés, solicito al ministro del Interior, quien es el jefe superior de Carabineros, que retire todos esos teléfonos celulares y los entregue para hacer la pericia correspondiente; de lo contrario, al final del día los siguen usando. Sería interesante hacerles las pericias correspondientes para ver en qué consistieron los parches. No sé qué preguntas habría que formularles a los peritos para saber qué objetivo tenían los parches, quién los puso, por qué lo hicieron y si cumplieron su fin.

El señor **COLOMÉS**.- Primero habría que determinar si se instalaron.

La señora **PARRA**, doña Andrea (Presidenta).- Sí, por eso acordamos oficiar a Carabineros. En realidad, no nos queda claro si efectivamente es un desvarío más del señor Smith o tenían el objetivo de extraer información física, que es lo que entendí que se podía hacer.

El señor **GUTIÉRREZ**.- Señora Presidenta, escuché que un general reconoció que le habían puesto esos parches.

La señora **PARRA**, doña Andrea (Presidenta).- Así es.

El señor **GUTIÉRREZ**.- Entonces, los parches fueron instalados.

La señora **PARRA**, doña Andrea (Presidenta).- Claramente.

El señor **COLOMÉS**.- Tal vez, él pasó su teléfono y desconoce el procedimiento que hicieron. A lo mejor, copiaron archivos. El peritaje informático revelará si ese eventual parche existe, si se instaló y funciona o si realmente tiene una aplicación espía como tal.

El señor **GUTIÉRREZ**.- Lo mejor es que se hagan las pericias.

La señora **PARRA**, doña Andrea (Presidenta).- El actual general director de la Unidad de Inteligencia, quien estuvo presente en la sesión anterior, señaló que él todavía tiene instalado un parche en su teléfono. En verdad, es curioso, por decirlo de alguna manera, o un contrasentido muy profundo haber escuchado eso. Nos sorprendimos, porque él es general…

El señor **COLOMÉS**.- Yo estaría preocupado.

La señora **PARRA**, doña Andrea (Presidenta).- Yo igual estaría preocupada.

El señor **GUTIÉRREZ**.- Señora Presidenta, por eso insisto en que sería bueno que el ministro del Interior adoptara las medidas correspondientes, porque él es el superior jerárquico de Carabineros. Él debería adoptar alguna medida respecto de los celulares que supuestamente tienen parches, los cuales no sabemos para qué sirven.

La señora **PARRA**, doña Andrea (Presidenta).- Lo solicitaremos, señor diputado.

Tiene la palabra el señor Pablo Viollier.

El señor **VIOLLIER**.- Señora Presidenta, junto con agradecer la posibilidad de exponer nuestros descargos, quiero reiterar la importancia que significa que hoy exista una especie de disciplina política respecto de Carabineros. Estamos frente a una institución que siente que tiene la Agencia para inventar pruebas, infectar celulares de imputados con *softwares* maliciosos, lamentarse públicamente de que esto se hace público y que en el futuro los imputados no van a caer en el *fishing* de Carabineros, oponerse físicamente a la realización de un procedimiento de incautación, solicitarle al exsubsecretario Aleuy que se aumente el período de retención de metadatos a dos años y que eso incluya todos los tipos de comunicaciones.

Entonces, dan cuenta de una institución que no se está sometiendo a un control democrático por parte del Ministerio del Interior y de la sociedad completa ni a los controles de nuestra propia legislación. Creo que en un Estado de derecho no hay espacio para una institución que se siente con una agencia para saltarse el control democrático de la sociedad y los controles al interior de un recinto penal. Es momento de que, como sociedad, le pongamos "el cascabel al gato" y que tanto Carabineros como la Fiscalía sean sometidos al control democrático, al control de nuestras instituciones y al control de nuestra legislación.

Hoy, el gobierno ha anunciado una modificación de nuestra legislación, de nuestro sistema de inteligencia. Esa es una muy buena oportunidad para proponer una modificación de la ley de Inteligencia en el sentido que propuse. Sin duda, sería una conclusión muy positiva para el informe de la Comisión.

Dentro de la política nacional de ciberseguridad, se encuentra como medida concreta la ratificación del Convenio de Budapest, que significará una actualización de la ley de Delito Informático. Es una muy buena posibilidad para concretar la recomendación que les hacíamos, en el sentido de prohibir la utilización de *malwares* por parte de instituciones del aparato del Estado.

Un señor **DIPUTADO**.- ¿Cómo se llama?

El señor **VIOLLIER**.- *Malware* es un código malicioso. Esta idea de que mando un correo falso diciendo que soy una tienda y le…

La señora **PARRA,** doña Andrea (Presidenta).- La práctica se llama *fishing.*

El señor **VIOLLIER.**- El programa se llama *malware.*

El señor **COLOMÉS.**- El *fishing* es cuando se envía una página falsa y uno introduce sus datos.

El señor **VIOLLIER.**- Es el uso fraudulento y engañoso de hacerme pasar por otra persona. Eso no lo puede hacer la policía dentro de un Estado de derecho. No puede engañar a sus ciudadanos para que voluntariamente entreguen su información sensible, como son sus usuarios y claves.

El señor **GUTIÉRREZ.**- En ese caso, sería una especie de ciberataque del Estado.

El señor **VIOLLIER.**- Así es. Es algo punible por la ley de delitos informáticos. Por lo tanto, la modificación de dicha ley, a propósito de la ratificación del Convenio de Budapest, es una muy buena oportunidad para que prohibamos esa actividad.

De manera que sería una conclusión muy positiva por parte de la Comisión que, en el fondo, cuando se ratifique el Convenio de Budapest y se modifique la ley de Delito Informático, se prohíba el uso de ese tipo de herramientas.

La señora **PARRA,** doña Andrea (Presidenta).- En nombre de la Comisión, agradezco la concurrencia y colaboración de nuestros invitados.

Estaremos en contacto con ustedes.

Por haber cumplido con su objeto, se levanta la sesión.

ALEJANDRO ZAMORA RODRÍGUEZ,
Redactor
Jefe Taquígrafos de Comisiones.

*****

El debate habido en esta sesión queda registrado en un archivo de audio digital, conforme a lo dispuesto en el artículo 256 del Reglamento[1].

Habiéndose cumplido el objeto de la presente sesión, se levantó a las 15:55 horas.

ÁLVARO HALABÍ DIUANA
Secretario de la Comisión

[1] Además, se encuentra disponible el registro audiovisual de esta sesión en el siguiente enlace: http://www.democraciaenvivo.cl/player.aspx?STREAMING=streaming.camara.cl:1935/cdtvvod&VODFILE=PROGC014261.mp4.