MATERIA: RECURSO DE PROTECCION
SECRETARIA: ESPECIAL
RECURRENTE: PEDRO HUICHALAF ROA Y OTROS
ABOGADO: PEDRO HUICHALAF ROA
RUT: [redacted]
RECURRIDO: ALEX GUILLERMO SMITH LEAY
RUT: [redacted]

EN LO PRINCIPAL: RECURSO DE PROTECCION

PRIMER OTROSI: MEDIDAS DE PROTECCION

SEGUNDO OTROSI: ACOMPAÑA DOCUMENTOS

TERCER OTROSI: SOLICITA OFICIOS

CUARTO OTROSI: PATROCINIO Y PODER

ILUSTRISIMA CORTE DE APELACIONES DE TEMUCO

PEDRO HUICHALAF ROA, abogado, rut [redacted], domiciliado en [redacted], [redacted] FERMIN JAVIER LEVIO LLANCAMIL, comerciante, rut [redacted], domiciliado [redacted] y MAURICIO ANDRES LLAITUL ACUM, técnico jurídico, rut [redacted], domiciliado en [redacted], a SSI respetuosamente decimos:

Que, encontrándonos dentro de plazo, tal como se indicará en su oportunidad, en virtud de lo establecido en el art. 20 de la Constitución Política de la República y en el Auto Acordado sobre tramitación y fallo del recurso de protección de las garantías constitucionales de 17 de julio de 2015 de la Corte Suprema, venimos en interponer acción de protección a favor de las siguientes personas que a continuación detallamos:

NOMBRE	RUT	DIRECCION	COMUNA
JAIME EDUARDO HUENCHULLÁN CAYUL, agricultor.	[redacted]	[redacted]	[redacted]
ERNESTO LINCOYAM LLAITUL PEZOA, estudiante universitario.	[redacted]	[redacted]	[redacted]
CLAUDIO ANTONIO LEIVA RIVERA, estudiante universitario.	[redacted]	[redacted]	[redacted]
MARTÍN DAMIÁN CURICHE CURIQUEO,	[redacted]	[redacted]	[redacted]

estudiante universitario.			
FIDEL LAUTARO TRANAMIL NAHUEL, Machi.	[redacted]	[redacted]	[redacted]
DAVID EDUARDO CID AEDO, sociólogo.	[redacted]	[redacted]	[redacted]
HÉCTOR JAVIER LLAITUL, CARRILLANCA, asistente social.	[redacted]	[redacted]	[redacted]
RODRIGO NAZARIO HUENCHULLÁN CAYUL, técnico en municipalidad de Ercilla.	[redacted]	[redacted]	[redacted]

y al mismo tiempo específicamente a nombre propio y respecto de cualquier otro habitante de Chile, y solicitamos que se tenga presentado en común, en contra de don ALEX GUILLERMO SMITH LEAY, RUT N° [redacted] Ingeniero Agrícola, cuyo domicilio es [redacted], quien por su actuar absolutamente fuera de la esfera de atribuciones que confiere la ley, en forma ilegal e inconstitucional, ha violentando y amenaza nuestros derechos básicos y garantías consagrados en la Constitución conforme con los hechos y el derecho que a continuación señalamos:

LOS HECHOS:

Para poder aclarar con exactitud la vulneración de derechos constitucionales respecto a las personas individualizadas a nombre de quien presentamos el presente recurso de protección (y la fecha en que se tuvieron conocimiento de estas vulneraciones) y por otro lado la posible amenaza de vulneración de derechos de quienes suscribimos (y al mismo tiempo la fecha en que tuvimos conocimiento de esta amenaza), es que debemos explicar en primer lugar los hechos fundantes separadamente.

En primer lugar explicaremos la situación de hecho respecto a personas a quienes presentamos a su favor el recurso de protección y en segundo lugar explicaremos los hechos fundantes de quienes suscribimos este recurso.

1) situaciones de hecho conducentes a verificar la vulneración de derechos constitucionales respecto de personas a nombre de quienes presentamos el presente recurso:

Es de público conocimiento que a fines de septiembre de 2017, en el marco de la denominada "Operación Huracán", se detuvieron a 8 comuneros mapuches, que corresponden a las personas individualizadas inicialmente como los afectados en sus derechos constitucionales, por parte de Carabineros de Chile quienes actuaron por orden solicitada por Ministerio Público.

En su oportunidad, el entonces jefe de la IX Zona Araucanía, general de Carabineros Christian Franzani Cifuentes, indicó (tal como lo consigna el medio

electrónico Radio Bío Bio)[1]... "a raíz de un sin número de órdenes de investigar **que maneja nuestro servicio de Inteligencia,** desde hace seis meses a la fecha se venían investigando diferentes hechos de violencia rural de carácter terrorista, y hoy se ha procedido a realizar diferentes allanamientos en la macrozona, entre la VIII y XIV región(…) todas estás personas están vinculadas de una u otra forma de acuerdo a los antecedentes y pruebas científicas, a diferentes delitos entre ellos quema de camiones e iglesias"...

Tras la detención de los comuneros, y ante el Juzgado de Garantía de Temuco, se les imputó el delito de "asociación ilícita terrorista".

El ministerio Público en esa instancia solicitó y se accedió por el Juez de Garantía, el plazo de 4 meses de investigación, ordenándose al mismo tiempo el secreto de la misma y se solicitó la prisión preventiva de los comuneros, la cual fue efectiva hasta que la Corte Suprema, el día 23 de octubre de 2017 decretó la libertad inmediata de los ocho comuneros mapuche detenidos.

De acuerdo a la resolución de la corte, la decisión tomada por la jueza de garantía de Temuco Luz Arancibia, tenía falta de fundamentos para justificar la medida cautelar. Sin perjuicio de esta medida, seguía la orden de investigar teniendo como imputados a los comuneros mapuches.

Es importante mencionar que la base de esta "Operación Huracán" y pruebas fundantes, fue realizada por acción de Carabineros bajo la Ley de Inteligencia, quien recopiló diversos antecedentes de los ocho comuneros mapuches basados en sus supuestos vinculados a la Coordinadora Arauco-Malleco (CAM) y a otras organizaciones de característica similares. Tras meses previos de seguimientos e intervenciones a los aparatos telefónicos de los comuneros (tal como se indicó en la audiencia en que fueron imputados), Carabineros entregó a la fiscalía el oficio 130, el cual contenía supuestas conversaciones vía WhatsApp y Telegram entre comuneros, en las que coordinaban eventuales acciones violentas.

El oficio 130 fue entregado por Carabineros a la fiscalía el 20 de septiembre de 2017 y en él se advertía, entre otros, que los comuneros preparaban un atentado en contra de la empresa de transportes Riquelme Correa, en las afueras de Temuco. Por ello, el Ministerio Público solicitó tres días después las órdenes de aprehensión en contra de los comuneros, las que fueron ejecutadas ese mismo 23 de septiembre. Tras ello, Carabineros hizo peritajes a los teléfonos celulares que requisó de los comuneros y emitió nuevos preinformes que avalaban la información de inteligencia que habían entregado inicialmente a través del oficio 130.

Mientras seguía en curso la investigación, el 25 de enero de este año, por trascendidos de investigación de prensa[2], y por información pública emanada de la Fiscalía, se indicó que este organismo había decidido cerrar la investigación "Operación Huracán" y abría otra investigación en contra de Carabineros. Esta situación se dio con

[1] Declaraciones disponible en la dirección http://www.biobiochile.cl/noticias/nacional/region-de-la-araucania/2017/09/23/detienen-a-6-comuneros-mapuche-presuntos-autores-de-atentados-en-la-araucania-y-los-rios.shtml

[2] Investigación disponible en https://www.biobiochile.cl/especial/noticias/reportajes/reportajes-reportajes/2018/01/25/fiscalia-cierra-operacion-huracan-y-abre-investigacion-en-contra-de-carabineros.shtml

la antesala de una querella en contra de Carabineros que presentó el viernes 19 de enero de 2018 Luis Arroyo, jefe de la Unidad de Delitos de Alta Complejidad de la fiscalía de Temuco. El libelo tiene relación con una arista de la Operación Huracán y en él, Arroyo da cuenta de supuestas pruebas falsas que le habría presentado Carabineros, mediante otro oficio, el 202, al Fiscal Nacional, Jorge Abott, para inculparlo en una eventual filtración de antecedentes del caso Huracán a los comuneros mapuches investigados.

Según se decribe en la querella, el Fiscal habría indicado que "Al parecer (los autores del oficio 202) persiguen crear un daño irreparable a mi imagen, credibilidad y seriedad profesional, dado el cargo que ostento, al igual que a la institución a la que pertenezco, quizás con la intención de hacerme a un lado de las investigaciones que dirijo y, a la vez, justificar el fracaso de sus operaciones investigativas".

Arroyo, a través Felipe González, fiscal adjunto a cargo de la Operación Huracán, había advertido, de manera reservada, los vicios del oficio 130 de Carabineros, ordenando tres peritajes para compararlos con los que había hecho la institución policial, los que finalmente arrojaron como conclusión un montaje en las pruebas contra los comuneros mapuches. El oficio 202, que involucra al fiscal con una supuesta filtración de antecedentes, también es visto en el Ministerio Público como un posible montaje contra Arroyo, dado sus cuestionamientos iniciales a los procedimientos de Carabineros.

Es así como en la querella del fiscal Arroyo, indica que el 26 de diciembre de 2017 él fue notificado de una investigación seguida contra la abogada asistente de la Fiscalía de Alta Complejidad de la Araucanía, doña Mónica Palma Martínez, por el presunto delito de obstrucción a la investigación, teniendo como base determinados antecedentes obtenidos al amparo de la Ley 19.974 sobre el Sistema de Inteligencia del Estado. Para sustentar dicha imputación se agrega oficio 202 donde aparece transcripción de supuestas conversaciones vía mensajería WhatsApp entre la abogada Palma Martínez y el Fiscal Arroyo.

Indica el Fiscal que tales supuestas comunicaciones habrían sido conocidas por Carabineros debido a la interceptación telefónica de la abogada Mónica Palma, autorizada por un miembro de la Itma. Corte de Apelaciones de Temuco, con fecha 25 de Octubre de 2017.

Al mismo tiempo, señala que además de texto, existirían fotografías de Arroyo y su familia que existirían en el teléfono celular de la abogada Palma Martínez y que supuestamente habrían sido enviadas por el Fiscal Arroyo a la abogada, lo que descarta de plano, mencionando la falsedad de estos antecedentes.

Con posterioridad, al momento de conocerse el cierre de la investigación, en declaraciones del fiscal Cristián Paredes, el jefe de Arroyo y González, a Radio Bío Bío indicó "Hoy la fiscalía ingresó al Tribunal de Garantía de Temuco un escrito comunicando el cierre de la investigación y la decisión de no perseverar en el procedimiento en la causa por asociación ilícita terrorista e incendio terrorista conocida policialmente como Operación Huracán". "Esta decisión fue tomada luego de recibir dos informes técnicos emanados de la Unidad Especializada en Lavado de Dinero, Delitos Económicos y Crimen Organizado (Uldeco) de la fiscalía nacional, que confirman la existencia de irregularidades que podrían ser constitutivas de delitos en los

preinformes e informes periciales informáticos practicados por el Laboratorio de Criminalística (Labocar) de Carabineros a los teléfonos incautados a los imputados en esta causa, el día 23 de septiembre", agregó.

Según dijo Paredes, "hemos constatado que hubo manipulación de la evidencia y que los archivos que contienen las supuestas conversaciones que inculpan a estas personas, pudieron haber sido artificialmente instalados en los equipos telefónicos después de que fueron incautados, ya que no corresponden ni al formato ni a la ubicación en la que se almacena la mensajería en los aparatos telefónicos".

"Estamos frente a un hecho gravísimo. Esta es la primera vez que esta fiscalía regional recibe una información de parte de Carabineros que se desarrolló íntegramente conforme al estatuto previsto en la Ley de Inteligencia, esto significa que se hizo con diligencias investigativas realizadas autónomamente por Carabineros y sin el control de los fiscales. En cuanto detectamos estas irregularidades, se instruyó la realización de peritajes para despejar estas dudas", agregó el fiscal Paredes.

La importancia de este hecho, en particular para los comuneros mapuches a nombre de quienes presentamos el presente recurso de protección, se basa en que a partir de este momento, a propósito del escrito presentado por Fiscalía ante Juez de Garantía de Temuco informando sobre la decisión en orden a cerrar la investigación con fecha 25 de enero de 2017,[3] es que por primera vez tienen conocimiento (debido al secreto que tenía la carpeta investigativa), respecto a que dentro de las medidas investigativas se encontraba el Oficio N° 130 de fecha 20 de septiembre de 201, suscrito por el Director Nacional de Inteligencia, Drogas e investigación Criminal de Carabineros de Chile, General Gonzalo Blú Rodriguez, en donde por invocación de la Ley de Inteligencia del Estado, habrían logrado la autorización por parte del Ministro de Corte de Apelaciones de Temuco, Sr. Aner Padilla Buzada, dos resoluciones, de fecha 9 de agosto de 2017 y el 07 de septiembre de 2017, para concretar diferentes medidas intrusivas, tendientes a recabar información respecto de personas o grupos que puedan estar involucrados en la planificación de atentados dentro del sector jurisdiccional de la citada Corte.

En dicho informe n°130, de información obtenida por personal de inteligencia de Carabineros, señala que se obtuvo por medios tecnológicos las comunicaciones realizadas a través de aplicaciones WhatsApp, Facebook, Telegram y correos electrónicos, entre distintos sujetos entre los que se indicaban los 8 comuneros mapuches del presente recurso de protección. El contenido de dichas conversaciones fue obtenido mediante la interceptación, recuperación y registro fidedigna de las misma, llevado a cabo por los sujetos indicados, las que se habían sido almacenadas desde el 1° de agosto de 2017 en adelante. En definitiva, el documento de inteligencia concluía que los sujetos indagados poseían información privilegiada, estando en conocimiento que sus teléfonos celulares se encontraban intervenidos.

Es importante señalar, por tanto, que sin perjuicio de eventuales responsabilidades administrativas y penales que hoy se encuentran en investigación, la DIPOLCAR (Dirección de Inteligencia Policial de Carabineros de Chile), utilizó medidas tecnológicas intrusivas con anterioridad a la autorización otorgada por el

[3] Copia del escrito que puede ser visualizado en https://es.scribd.com/document/370004489/17025806#from_embed

Ministro de Corte de Apelaciones en conformidad a las normas de la Ley de Inteligencia del Estado.

Es relevante al mismo tiempo indicar que en conformidad a lo que se indica en el escrito de decisión de no perseverar en la investigación de la "Operación Huracán", la Fiscalía solicitó diversos informes periciales de informática forense confeccionados por el Departamento de Criminalística sección Temuco del Laboratorio Criminalística de Carabineros de Chile, en donde se señala uso de software antorcha y existencia de diversos archivos con extensión "txt" en carpetas de aplicaciones de WhatsApp y telegram, indicando en algunos informes la existencia de dichos archivos en unos celulares y en otros informes, no mencionando la existencia de los mismos en los mismos celulares periciados.

Es por lo mismo, y según se lee en escrito de Fiscalía, considerando el principio de objetividad y la necesidad de tener claridad respecto a la información contenida en los dispositivos electrónicos, como asimismo el contar con opiniones distintas destinadas a una investigación más profunda y eficiente, es que con fecha 11 de diciembre de 2017, se remitió a la Unidad Especializada en Lavado de Dinero, Delitos Informáticos, Medioambientales y Crimen Organizado de la Fiscalía Nacional, en el cual se solicitó la extracción, revisión y análisis de la información relativa a mensajería contenida en la evidencia individualizada en dicho informe, pidiéndose, además, determinar la estructura y extensión, ubicación en el dispositivo, fecha de registro, metadatos de los antecedentes, así como cualquier información, datos y elementos asociados.

De esta diligencia se obtuvo respuesta por medio de oficio N°1032 de 11 de diciembre de 2017 y en la cual se pudo constatar la existencia de algunos archivos que no guardarían relación con las formas en las que se almacenan las mensajerías al interior de los dispositivos telefónicos, por lo que en sus conclusiones se resuelve que se identificaron 05 archivos de extensión TXT que no corresponderían a los archivos de mensajería, sino que se tratarían de archivos de texto plano, es decir, formado exclusivamente por texto, sin ningún formato. Indica además que estos archivos no contienen TimeStamp (marca temporal), ni la estructura de un archivo exportado de la aplicación de mensajería a otra. Se logró identificar que, en uno de los teléfonos de los comuneros mapuches, se encontraron cuatro archivos con similar nombre, contenido y registro de fecha de creación, con distintas ubicaciones en la memoria del teléfono, lo cual se estima como irregular, ya que las aplicaciones de mensajería crean su propio directorio para almacenar los archivos que generan.

No conforme con lo anterior, Fiscalía solicitó una nueva pericia informática a la Unidad Especializada en Lavado de Dinero, Delitos Informáticos, Medioambientales y Crimen Organizado de la Fiscalía Nacional y con fecha 23 de enero de 2018 se recibe oficio en que se informa que sólo dos de los equipos telefónicos cuentan con aplicaciones de mensajería instalada al interior del equipo telefónico. Además, se establece que tres de los archivos de formato TXT encontrados al interior del equipo telefónico de Martín Curiche Curiqueo, tienen fecha de registro en el equipo posterior a la fecha de incautación. Agrega que los archivos de supuesta mensajería no reúnen las características ni condiciones de elementos generados ni exportados desde los aplicativos de mensajería instantánea (WhatsApp, Telegram y Facebook Messenger) ni tampoco del tipo SMS o cualquier tipo de mensajería instantánea común.

"Es por estas razones que, al haberse aportado por parte de funcionarios de Carabineros de Chile información y antecedentes de cargo que presentan múltiples anomalías e irregularidades, hacen dudar fundadamente de su veracidad y autenticidad y se ve impedido de continuar con la prosecución de la investigación criminal de manera tal que comunicó la adopción de la decisión de no perseverar en la investigación", concluyó.

Tras ello, el Juez de Garantía de Temuco fijó fecha de audiencia el viernes 09 de febrero recién pasado y acogió una petición de la Fiscalía para cerrar la investigación y su decisión de no perseverar en la investigación por la quema de decenas de camiones, sobre la base de que la Policía de Carabineros falsificó pruebas para acusar a dirigentes mapuches radicales. También el juez rechazó una petición del Gobierno para decretar la reapertura de la investigación y determinó también sobreseer de manera definitiva a los ocho comuneros imputados en la llamada "Operación Huracán".

Ahora bien, lo relevante de los hechos antes descritos, radica en que con la solicitud al momento del cierre de la investigación y decisión de no perseveración, (y no antes por existir decretado el secreto de la investigación) es que por primera vez ,este viernes 09 de febrero, en forma concreta los comuneros mapuche, a nombre de los cuales se presenta este recurso de protección, pudieron saber que sus teléfonos móviles, y con ello sus cuentas de correo y aplicaciones de mensajería instantánea WhatsApp, Telegram y Facebook Messenger (en los casos correspondientes que tenían unas u otras aplicaciones instaladas), fueron interceptadas por un software utilizado por DIPOLCAR.

Consecuencialmente a este hecho y en virtud de las atribuciones de investigación por parte del Ministerio Público, y debido a la presunta existencia de inconsistencias en las pruebas aportadas por Carabineros, se inició una investigación contra nueve efectivos de carabineros y un civil que son actualmente indagados por presuntos delitos de falsificación de instrumento público y obstrucción a la investigación.

Es relevante manifestar que producto de esta investigación se realizaron sendos allanamientos e incautaciones de equipos, tanto de dispositivos, computadores e imposición de sellos en servidores ubicados en instalaciones de DIPOLCAR en la ciudad de Temuco, como también en el domicilio de un particular no uniformado, en virtud del cual operaron las mismas medidas realizadas todas por funcionarios de Policía de Investigaciones, encomendadas por Fiscalía.

Es en este punto que llamamos la atención, porque a propósito de esta investigación de la "Operación Huracán" y de la posterior investigación por delitos de falsificación de instrumento público y obstrucción a la investigación iniciada por el Ministerio Público, públicamente y por primera vez en un proceso judicial surge la figura de Alex Guillermo Smith Leay, el civil no uniformado.

Unos días antes, el día 03 de febrero de este año, a través de reportajes especial realizado por periodistas del diario La Tercera, cuyo título es "Antorcha 3.0: La mano del controvertido "hacker" tras la Operación Huracán", se informa profusamente sobre la existencia de un software "capaz no sólo de intervenir celulares sino que también de ocupar un router para establecer la presencia de personas en un determinado lugar es la

creación de un ingeniero del Inacap, apodado "el profesor", que la Fiscalía ha puesto en entredicho y que la ha enfrentado con Carabineros a quienes acusa de manipular pruebas para inculpar a supuestos implicados en atentados en La Araucanía", tal como se indica en el reportaje antes mencionado[4].

Según se informe por este medio, en Carabineros se le llama "el profesor". Es el apodo con que personal de inteligencia de Temuco se refiere a Alex Smith Leay, el ingeniero agrícola y forestal -estudió en forma paralela ambas carreras en diurno y vespertino en Inacap-, quien asegura que diseñó y desarrolló el software -que llama "Antorcha"- que supuestamente intercepta conversaciones de WhatsApp y Telegram, cuya legitimidad puso en jaque la Operación Huracán.

Continuando con esta fuente periodística, se indica que el propio ingeniero Alex Smith quien hizo pública su colaboración con Carabineros el pasado 28 de noviembre en su Facebook donde posteó que "empecé en un nuevo empleo en Carabineros de Chile". El jueves 01 de febrero del presente año, cuando ya se hizo público que era el diseñador del controvertido software que avalaba las pruebas de Carabineros en la Operación Huracán, el ingeniero cerró su Facebook.

Uno de los puntos relevantes informados es que coincidentemente también el 01 de febrero de este año desapareció la página web donde supuestamente personal de Inteligencia de Temuco almacenaba información del software denominado al interior de la policía uniformada como "Antorcha" en sus versiones 1.0, 2.0 y 3.0.

Se indica que cercanos a Smith sostienen que desconocían su faceta al interior de Carabineros. Menos que en agosto de 2017 había creado el programa "Antorcha 1.0" -en alusión a su intención de poner "luz en la oscuridad"- para interceptar los mensajes de la agrupación terrorista que supuestamente lideraba Llaitul.

Pero "el profesor" era informalmente parte de Inteligencia de Carabineros desde enero del año 2017. Su nexo fue un oficial del Laboratorio de Criminalística de Carabineros, al que había capacitado y quien lo invitó a ayudar en algunos temas, dada su afición por lo informático y su diplomado en tecnología.

Se informó que la Fiscalía ya dispone la información de que a mediados del año pasado a Smith le habrían solicitado crear un software para interceptar celulares y poder determinar quiénes estaban detrás de los atentados en La Araucanía.

En Carabineros, en tanto, sostienen que existe una aplicación similar que ocupa la inteligencia de Israel, pero que adquirirla sería demasiado costosa. El ingeniero -defienden- la hizo gratis y demoró un mes. "Lo hizo porque le gustaba el reconocimiento que la policía hacía de su labor", sostuvo un cercano a Smith, quien había elaborado más de 100 reportes de inteligencia antes de que se formalizara su contrato grado 5 como personal contratado por resolución en Carabineros, con un sueldo de $1.400.000 líquido, aproximadamente.

Entre las colaboraciones de Smith a la policía uniformada incluso lo sindican como uno de los funcionarios que ha estado trabajando, con un equipo de Dipolcar en

[4] Reportaje disponible en versión digital en http://www.latercera.com/reportajes/noticia/antorcha-3-0-la-mano-del-controvertido-hacker-tras-la-operacion-huracan/56009/

Santiago, en pesquisas para esclarecer quién está tras la bomba que fue enviada a la casa del presidente del directorio de Codelco, Óscar Landerretche, en enero de 2017.

La participación del ya polémico ingeniero en otras investigaciones al amparo de la Ley de Inteligencia tomó mayor relevancia cuando la Fiscalía hizo público que otros casos como el del ataque a 29 camiones que tuvo lugar en San José de la Mariquina el 28 de agosto del año pasado también pudo ser objeto de pruebas falseadas.

Desde la misma institución explican que el software no funciona con las aplicaciones -como WhatsApp o mensajería de Telegram-, por el contrario, el programa se inserta al teléfono, lo que se puede hacer mediante un correo o mensaje que se envía al blanco de la pesquisa. Luego de enviado, como una suerte de "virus", todas las actividades que se realicen en el celular quedarán registradas por medio de un "efecto espejo" que va guardando los datos que se generen, pero no hace una copia de la aplicación.

El software, explican las mismas fuentes, funciona bajo el principio de los Keylogger, es decir, que se encarga de registrar las pulsaciones que se realizan desde el teclado del aparato para luego guardarlas en una carpeta que se envía por internet. Al mismo tiempo, en la institución aseguran que la aplicación de Smith está hecha para no ser rastreada, por lo tanto, va generando cambios en las fechas en que se realizaron los mensajes. Por eso mismo, explican, no sería extraño que existan mensajes que desde el programa tengan una fecha distinta a la que efectivamente se realizó.

Estos antecedentes respecto al funcionamiento del controvertido software están contenidos en el "informe 202" de Inteligencia que se entregó al Ministerio Público como parte de las pericias de la Operación Huracán.

En la institución uniformada se sostiene también que Smith ha ido perfeccionando el software: la primera versión 1.0 del programa no habría logrado identificar fechas ni horas y son las que se usaron en la Operación Huracán. Sólo la versión de "Antorcha 3.0" lograría no sólo capturar el texto, sino además imágenes. Sin embargo, el informe 130 -en que se desclasifican pruebas para las detenciones de esta operación- sí incluye la extracción de imágenes, fechas y horas de las conversaciones.

Sin considerar estos hechos informados gracias a un trabajo investigativo de periodistas, también existe información aparecida públicamente en otro reportaje del Diario La Tercera del día 06 de febrero de 2018[5], donde se transcribe parte de la declaración prestada por Alex Smith el día 30 de enero ante la Fiscalía, por la investigación que dio inicio el Ministerio Público a raíz de peritajes realizados y que verificaron una supuesta manipulación en la prueba obtenida por Carabineros bajo las reservas de la Ley de Inteligencia. Por nuestra parte, reproduciremos parte de esta entrevista con respecto a los hechos fundantes del presente recurso de protección.

Sobre sus especialidades en materia informática, describe que "soy ingeniero forestal e ingeniero agrícola de Inacap, estudié paralelamente las dos carreras, una diurna y la otra vespertina. Además, tengo MBA en Administración en Empresas de la

[5] Artículo de prensa del Diario La Tercera disponible en versión web http://www.latercera.com/nacional/noticia/la-declaracion-del-hacker-creo-antorcha-software-la-operacion-huracan-no-busco-dinero-reconocimiento-carabineros-basta/59218/

Universidad Santo Tomás de Temuco, que obtuve el año 2015. Tengo diplomado en seguridad informática de la Universidad Mayor, entre otros, pues tengo aproximadamente ocho diplomados de diferentes casas de estudios y en distintas áreas, desde la administración de empresas a la informática (…) He estudiado muchas cosas, pues soy muy inquieto".

Continuando con su declaración señala que "Inacap me contrató antes de que terminara de estudiar el año 1998, me hice cargo de un laboratorio de informática y llegué a ser jefe de carrera. Mientras era jefe de carrera ya hacía clases en Inacap capacitación. Comencé impartiendo cursos en el área forestal e informática. En el año 2009 me fui al CFT y al IP Santo Tomás como docente, luego comencé a hacer clases en la Universidad Santo Tomás, como profesor de ingeniería comercial. Hasta la fecha soy docente en la Universidad Santo Tomás, Mayor y Católica de Temuco, mis áreas de docencia son las tecnologías de la información, computación, software de administración y otros. Imparto mis clases en las carreras de derecho, ingeniería comercial, medicina, terapia ocupacional", explica.

"Debido al hecho de que yo les hacía cursos a los Carabineros, y ya me conocían, en enero de 2017 me contacta el Capitán Osses y me pide ayuda en un asunto asociado al caso Landerretche. Concurrí a Santiago a apoyar para realizar el peritaje asociado con un comunicado. Unos meses antes yo había conocido al Capitán Osses en uno de los tantos cursos que había impartido, seguramente él se consiguió mi teléfono, me llamó y me solicitó ayuda. Le presté la ayuda que me pidió en forma ad honorem", dijo.

Acto seguido agrega que "mi ayuda se extendió por una semana aproximadamente. Desconozco si mi ayuda se reflejó en un informe, pero sé que el trabajo les sirvió porque aún seguimos trabajando y entiendo que las personas asociadas al comunicado están identificadas. En el computador que me incautaron está la información asociada a este asunto".

De la forma que he relatado, y en este contexto, fue que me ofrecieron ser contratado CPR grado 5, a contar del 8 de octubre de 2017. Recuerdo que fue en esa época, pues ya había terminado algunas horas de clases que estaba realizando. Una vez contratado por Carabineros, mi función principal era seguimiento de las redes sociales. Tenía una jornada de 44 horas semanales, de 08:00 a 13:00 y de 16:00 a 20:00".

Hasta ese entonces, el profesor tenía una función clara: "el seguimiento de blancos investigativos a través de redes sociales. Lo anterior consistía en obtener datos de fuentes abiertas de diferentes personas, no sólo de la región de la Araucanía, pues trabajábamos para las fiscalías de Iquique hasta Los Ríos. Siempre trabajé bajo la dirección del Capitán Leonardo Osses, él era quien me indicaba qué blancos investigativos íbamos a seguir. Mi trabajo se concretaba a través de presentaciones Power Point y excepcionalmente documentos Word. Mis reportes siempre iban dirigidos al Capitán Osses. Los reportes se entregaban a través de diferentes vías dependiendo de la urgencia, podía ser WhatsApp o correo electrónico".

"Además de lo que acabo de contar, en conjunto con Carabineros desarrollé varias aplicaciones a contar de julio de 2017. Quiero agregar que a principios de julio el Capitán Osses, el mayor Patricio Marín y el Coronel Teuber, en primera instancia por

separado, y luego en una reunión conjunta, me comentaron que existía la posibilidad de que me contrataran como CPR, pero para ello debían cumplirse varios trámites y dentro de unos meses podría procederse a la contratación. Nunca estuve seguro de trabajar en Carabineros sino hasta el 8 de octubre, no obstante que ya existían conversaciones con anterioridad para llegar a trabajar con ellos. Hasta antes del 8 de octubre, trabajaba para Carabineros los tiempos que podía, como un favor. Sólo a contar del 8 de octubre comencé regularmente a trabajar con Carabineros", dijo.

"Debo precisar que la aplicación era desarrollada sólo por mí, y que los funcionarios de Carabineros simplemente me indicaban qué era lo que necesitaban. La aplicación desarrollada entregaba reportes que eran descargados directamente por Carabineros. La aplicación se abría en el computador y la primera acción consistía en escoger entre Android o OIS, luego debían ingresarse algunas variables tales como correo electrónico, imei, número de teléfono, simcard. Lo indispensable era tener el correo electrónico sincronizado con teléfono. Para obtener este dato correspondía a la labor de investigación de Carabineros", aseguró a Fiscalía.

Agregó que "una vez ingresadas las variables, el servidor de la UIOE enviaba un correo electrónico al teléfono que se quería intervenir. Todo ello con orden judicial. El correo enviado contaminaba el teléfono (…) Los correos electrónicos enviados eran promociones y bastaba con estos llegaran al correo a la bandeja de entrada para infectar el aparato. Los correos estaban diseñados para pasar la barrera del spam".

Según Smith ni siquiera era necesario abrir el correo para que el dispositivo fuera infectado. "No era necesario que el usuario abriera el correo que se le había enviado. Sólo bastaba con que ingresara a la bandeja y luego el usuario utilizara aplicaciones tales como whatsapp y telegram. Esta información se podía observar en otro aparato".

Confiesa que existían ciertas limitaciones en esa primera versión que se usa para Operación Huracán: "no podía hacerse con más de 10 teléfonos y además si el usuario escribía muy rápido tampoco lo captaba. El sistema fue evolucionando y fue denominado "antorcha", inicialmente sólo capturaba texto. La información que se captaba se almacenaba en el servidor de la UIOE, en formato html".

Según el testimonio de Smith, Antorcha 1.0 sólo capturaba textos. Sin embargo, en el informe de inteligencia 130 de Carabineros aparecen fotografías extraídas supuestamente de los celulares de los imputados en las que se jactan de los ataques en medios de la supuestas conversaciones capturadas por la aplicación.

Tal como se indica en la nota y sólo confirmando la opinión del periodista redactor del artículo, la autorización judicial que dio la Corte de Apelaciones de Temuco bajo la Ley de Inteligencia nunca permite o autoriza diligencias para infectar o intervenir correos electrónicos como asegura Smith lo hicieron en Operación Huracán.

"El sistema fue evolucionando y fue denominado "Antorcha", inicialmente capturaba solo el "texto". La información que se captaba se almacenaba en el servidor UIOE, en formato HTML. Yo no operaba la aplicación. Yo la diseñé y la entregué conforme a lo que me solicitaron y eso fue mejorando con el tiempo. El cabo Olave era quien descargaba la información. Inicialmente copiaba la información desde el servidor

a un documento Word. El servidor se denominó airs.cl y su clave era 478712000. El dominio se compró en Nic Chile, ignoro el nombre de a quién se le compró".

La inspiración que habría tenido era un programa que existe un servicio de inteligencia de otros países como Israel, "pero no se trata de una herramienta que se pueda adquirir en el mercado. Yo me aboque a desarrollarla en mis ratos libres, sin cobrar nada, tardando cerca de un mes en crear un primer prototipo operativo. Quiero hacer presente que realicé esta labor pues es mi pasión es la programación y mi intención es marcar un sello".

El ingeniero forestal y agrícola prosigue asegurando que "mi participación en la Operación Huracán se produjo luego de las detenciones. Antes de esa fecha me dediqué a monitorear las redes por fuentes abiertas y a desarrollar la aplicación que permitía la creación del espejo de los blancos investigativos. Pero en esta labor no tenía conciencia de que se estaba preparando una operación, esa no era mi labor (…) yo no participé en las pericias. No tuve contacto con los teléfonos. Tampoco operé ningún equipo. Mi labor sólo fue de asesoría. Todos estaban muy nerviosos y yo estaba calmado. Por eso los orienté".

Hace alusión a sus supuestas labores en El Robo del Siglo. "Mientras estuvieron trabajando los peritos en la UIOE, yo asistía en diferentes horarios a la UIOE y estuve trabajando en otros casos. El principal fue el denominado "robo del siglo", realizando las mismas labores que ya he comentado, es decir, mejorar la aplicación "Antorcha" y otros en que estábamos trabajando".

Éste punto es relevante a considerar debido a que señala que la aplicación antorcha fue utilizada por casos distintos a la investigación por delitos terroristas y ajenos a medidas intrusivas autorizadas por la ley de Inteligencia del Estado, según es nuestro entender.

"La herramienta Antorcha nunca permitió, en ninguna de sus versiones, recuperar conversaciones anteriores. Sólo era un espejo de lo que se escribía, inicialmente, ni siquiera se podía obtener día y hora de la conversación. Sólo lo que el usuario del teléfono intervenido escribía y el apodo del interlocutor del teléfono intervenido", declaró Smith sobre la versión de la aplicación usada en Huracán.

También dijo que la primera versión tenía limitaciones como poder funcionar sólo con 10 celulares a la vez y si "el usuario escribía muy rápido no se captaba la conversación".

En lo anterior se evidencia una contradicción del ingeniero pues el informe 130 de Inteligencia de Carabineros con que se pide a la Corte de Apelaciones interceptar conversaciones, y que fue entregado por el general de Inteligencia Gonzalo Blu a la Fiscalía, contiene conversaciones anteriores a la fecha de la autorización judicial que la dio el ministro Aner Padilla el 9 de agosto del año pasado.

Acto seguido, "el profesor" explica que "en esta primera versión el día y hora de la conversación se obtenía por el reporte del servidor. Era labor de los investigadores establecer a quienes correspondían tales apodos. La versión de "Antorcha" que se utilizó en la operación Huracán fue la primera y comenzó a utilizarse en agosto de

2017" y agrega que Antorcha tiene cuatro versiones (1.0, 2.0, 3.0 y 4.0) y lo que ha ido cambiando es la interfaz.

Siguiendo con los mismos antecedentes, según consta en otro artículo publicado por el Diario La Tercera[6], se transcribe otra declaración de Alex Smith en la que menciona "Personalmente, nunca he mostrado cómo funciona el sistema que acabo de explicar a un fiscal de La Araucanía; sin embargo, sí se lo he mostrado a un fiscal de Rancagua y al fiscal militar de Iquique, hace poco tiempo. No se lo demostré al ministro de la Corte de Apelaciones de Temuco, que autorizó su uso en la Novena Región".

Esta declaración entregada en calidad de imputado por el ingeniero Alex Smith al persecutor regional de La Araucanía, Cristián Paredes, en la investigación por la presunta manipulación de evidencia en la Operación Huracán, abrió una interrogante en el Ministerio Público: ¿Qué pasó en esa prueba? ¿Funcionó realmente el programa que habría desarrollado Smith, llamado "Antorcha" y que permitía interceptar conversaciones de WhatsApp y Telegram?

El fiscal que hizo la prueba con el ingeniero fue el persecutor de Rancagua Sergio Moya, quien consultó al informático cómo operaba el software.

Para aclarar las dudas, Paredes solicitó a Sergio Moya que elaborara un informe, comunicándole cómo fue el test del programa que hizo con "el profesor" (Smith).

El fiscal Moya accedió a la solicitud y remitió el análisis al persecutor regional de La Araucanía, quien mantiene bajo reserva este documento por 40 días. En el texto se da cuenta de cómo se desarrolló la prueba y sus resultados. No obstante, el contenido del documento se mantiene en estricto secreto.

Sin perjuicio de lo transcrito y considerando que la fuente, como se indicó, es una posible copia de la declaración realizada por Alex Smith a fiscalía (lo que podría generar dudas respecto a la veracidad de haber realizado esas declaraciones), con posterioridad ha sido el propio Alex Smith quien ha hecho declaraciones a diversos medios de prensa, escritos y de televisión, señalando claramente los hechos de haber sido el creador del software "antorcha", y ha descrito profusamente su modo de operar y funcionalidad, es decir, acceder e intervenir correos electrónicos y aplicaciones de mensajería instantánea sin autorización previa de los afectados.

Es así como por ejemplo este lunes 12 de febrero, sale publicada entrevista otorgada para el Diario "El Mercurio"[7] , en donde Alex Smith explicó cómo opera su aplicación "Antorcha" y qué resultados se pueden obtener con ella. A continuación se transcribe parte de su declaración a objeto de tener acreditados hechos fundantes del presente recurso de protección.

Lo primero que precisa es que él no creó un software, "eso tarda muchos años", dice, sino que una aplicación. Esta es la razón por la cual se demoró poco tiempo. Las

[6] Nota de prensa disponible en versión digital http://www.latercera.com/nacional/noticia/paredes-pidio-informe-fiscal-rancagua-prueba-antorcha/62070/

[7] Artículo disponible en versión web http://www.elmercurio.com/blogs/2018/02/12/58005/No-hubo-manipulacion-por-parte-de-Carabineros-hubo-errores-de-programacion-y-de-protocolos-de-peritajes.aspx

primeras pruebas se realizaron en julio y se usaron alrededor de 100 celulares que con el virus se echaron a perder, "hasta que se mejoró".

Fue un día que estaba trabajando en la oficina de inteligencia y vio el logo de esa unidad -que es una antorcha-que decidió bautizar de esa manera su creación.

En entrevista con "El Mercurio", Smith explicó ayer cómo opera su aplicación "Antorcha" y qué resultados se pueden obtener con ella. Precisó que para extraer interceptación de un "blanco" enviaba un correo electrónico que contenía un malware o programa espía, pero también intentaba phising mediante un link, que permite capturar contraseñas, y un "código espejo" que posibilita interceptar comunicaciones por digitación, es decir, cuando la persona va escribiendo en su dispositivo.

A veces ocurría que en el blanco no abría el correo y no era posible la descarga del malware ; otras, "caían" con los tres sistemas de captura de contraseñas y mensajería. Por lo que a su juicio, un mensaje podía estar localizado en una más de una carpeta de aplicación.

-¿Cómo funciona su aplicación?

"El phishing es para obtener las claves (contraseñas) de ellos (los "blancos"), si no leían el link, no teníamos nada, pero al abrir el correo (malware), el código bajaba no más".

-¿Podían caer las tres juntas?

"Sí. Primero era phishing, adornado con una foto, bonito, para obtener contraseñas, es lo mismo que hacen para las estafas bancarias. El espejo (digitación) y el malware o los famosos Txt. El phishing es un link alojado en un servidor, yo tengo una página bonita para que tú pongas la clave (contraseña). Pero no siempre resultaban las tres".

No conforme con esta entrevista, Alex Smith también entregó su versión al periodista Emilio Sutherland, lo que fue presentado como reportaje de Canal 13 el día domingo 11 Febrero 2018, quien conversó con el hombre clave en la cuestionada Operación Huracán de Carabineros. En dicha nota televisiva, la cual se encuentra disponible para su visualización en sitio web de Canal 13[8], se incorpora el siguiente resumen: “Este es el relato y los descargos del ingeniero que creó el software que habría permitido extraer los supuestos mensajes de Whatsaap que involucraron a comuneros mapuches en atentados incendiarios”.

En esta entrevista televisiva nuevamente ratifica que es el desarrollador de la aplicación llamada “Antorcha” (que en sentido técnico es un software), mencionando expresamente, hecho que es absolutamente relevante para efectos de fundar el presente recurso de protección, que este software fue el utilizado en el “operativo Huracán”, siendo intervenidos utilizados por este programa, los dispositivos móviles, correos electrónicos y aplicaciones de mensajería instantánea de los comuneros mapuches inicialmente inculpados y que corresponden específicamente a las personas a nombre de las cuales se presenta este recurso de protección, recibiendo según detalla en la

[8] Video disponible para su visualización en http://www.t13.cl/videos/nacional/video-relato-del-acusado-montaje-operacion-huracan

entrevista, múltiples mensajes, correos, de diversas personas que lo denominan “el sapo de la DIPOLCAR”.

A modo de resumen, luego de explicar con detalle todos los hechos que consideramos relevantes y fundantes para el presente recurso de protección, tenemos que:

- Existe un reconocimiento expreso que Alex Guillermo Smith Leay desarrolló una aplicación que lo denominó “antorcha”y cuya propiedad intelectual es de este individuo, toda vez que la confeccionó personalmente y la facilitó a terceros (en este caso a Carabineros) a título gratuito para su uso para labores de investigación de la DIPOLCAR. No existe constancia de haber facilitado el programa a terceros, pero tampoco existe certeza de que no lo haya realizado.

- Se constata que desarrolló el software con anterioridad a ser contratado a contrata por Carabineros (8 de octubre de 2017), en donde su rol era de asesor informático. Por lo tanto consta con ello que el programa no ha sido adquirido por Carabineros, no existe compra pública asociada a esta aplicación y por tanto la institución no tiene derecho alguno sobre el desarrollo de este software.

- El programa “antorcha” consistía en una unión de sistemas, conformado por una aplicación que era enviado por correo electrónico a un tercero, el cual le daba acceso y control sobre el dispositivo, por una parte, y además un servicio web alojado en un servidor, en donde se analizaba el resultado de la instalación de la aplicación y se almacenaba información privada de los terceros “infectados” por el programa informático, tales como conversaciones, imágenes, documentos, etc.

- Queda completamente acreditado que el único objetivo y funcionalidad del programa “antorcha”, no existiendo ninguna otra razón distinta de uso o desarrollo, era la interceptación de las comunicaciones privadas y acceso a dispositivos móviles de los terceros afectados. Por tanto, la única naturaleza es el espionaje informático.

- Quedo establecido que los terceros víctimas de la aplicación de este software de espionaje (con excepción de aquellos que probaban la funcionalidad aceptando su instalación, tal como ocurre con el fiscal de Rancagua), no tenían conocimiento de este programa y de sus efectos, y de modo alguno autorizaban expresamente su utilización e instalación, ni mucho menos el acceso a sus dispositivos móviles y por consecuencia, intervención en sus comunicaciones y obtención de conversaciones privadas generadas por aplicaciones de mensajería instantánea como WhatsApp, telegram y Facebook Messenger. Esto se ratifica por parte del mismo Alex Smith quien señala que el procedimiento “es lo mismo que hacen para las estafas bancarias”, toda vez que se enviaba un correo utilizando la técnica de “phishing”, es decir, suplantando el contenido y enlaces de un correo, engañando al receptor del mensaje para que al abrir el correo (e incluso sin necesidad de abrir el correo según declaraciones de Alex Smith), y siguiendo un link, descargara el archivo “malware” o programa espía, sin conocimiento o advertencia previa de este hecho.

- Queda establecido el hecho que realizó varias versiones del software “antorcha”, en virtud del cuál cada nueva versión agregaba más herramientas eficaces e intrusivas

sobre los llamados “blancos” o terceros afectados con la implantación del software espía.

- Queda completamente acreditado que se utilizó el software “antorcha” y son víctimas de su uso los 8 comuneros mapuches a favor de los que se presenta este recurso de protección, los que nunca supieron ni aceptaron la instalación de programa espía, ni dieron el consentimiento para la interceptación de sus comunicaciones privadas ni el control de sus dispositivos móviles.

- Queda constancia para efectos de plazo de interposición del presente recurso, los comuneros supieron de la existencia del programa espía, sus efectos y el nombre del creador del software, es decir, Alex Smith, el mismo día en el cual comparecieron ante el Juez de Garantía de Temuco , es decir el día viernes 09 de febrero recién pasado, juez que en definitiva acogió la petición de la Fiscalía para cerrar la investigación y su decisión de no perseverar en la investigación por la quema de decenas de camiones y liberó con ello el secreto de la investigación que impedía conocer estos detalles. Es importante recalcar que, tal como se acredita en los antecedentes, incluso antes de que DIPLOCAR invocara la Ley de Inteligencia del Estado y contara con autorización de Ministro de Corte de Apelaciones de Temuco, fueron infectados por el programa “antorcha” (toda vez que existe registros de conversaciones con anterioridad a la fecha de la autorización de los denominados “procedimientos especiales de obtención de la información” indicados en Ley antes indicada. En estricto rigor los derechos constitucionales que sufrieron privación y perturbación (y que más adelante en el presente escrito se explicarán) comenzaron a ser vulnerados desde antes de la autorización del ministro de Corte (recordemos que se logró 2 autorizaciones cuyas fechas de autorización fue 9 de agosto de 2017 y el 07 de septiembre de 2017) , pero sólo tuvieron conocimiento efectivo de la vulneración este viernes 09 de febrero, (luego del levantamiento de secreto de la investigación), por lo que se entiende presentado el recurso dentro de los plazos legales y efectivamente acreditado.

2) situaciones de hecho conducentes a verificar la vulneración de derechos constitucionales respecto de personas a nombre de quienes presentamos el presente recurso a nombre propio:

Es importante comenzar señalando que las personas quienes presentamos el presente recurso a nombre propio, lo hacemos en relación con la existencia de amenaza de las garantías constitucionales que se explicarán en extenso, cuando nos referiremos a las consideraciones de derecho fundantes del presente recurso. Por lo tanto, indicaremos a continuación las consideraciones de hecho propiamente tal que justifican plenamente la presente acción.

Al igual que los comuneros mapuches a nombre de los cuales presentamos este recurso, los firmantes de este recurso tuvimos conocimiento público el viernes 09 de febrero recién pasado, cuando el Juez de Garantía de Temuco acogió la petición de la Fiscalía para cerrar la investigación y su decisión de no perseverar en la investigación en el marco de la “operación Huracán”, de todos los antecedentes existentes luego del levantamiento del secreto de la investigación correspondiente.

Nos interiorizamos, por tanto, de todos los antecedentes de hecho que volvemos a indicar y que son fundantes a favor de comuneros mapuches de este recurso y que por economía procesal solicitamos se tenga nuevamente considerados, sin necesidad de volver a señalarlos, pero que en conclusión se resume que supimos de la existencia del llamado software "antorcha", cuyo desarrollador es Alex Smith.

Sin perjuicio de lo anterior, y tal como se indicó anteriormente, también pudimos observar como Alex Smith entregó su versión al periodista Emilio Sutherland, exhibido en televisión con el título de reportaje de Canal 13. En dicha nota televisiva, exhibida el domingo 11 febrero 2018, la cual se encuentra disponible para su visualización en sitio web de Canal 13[9], se incorpora el siguiente resumen: "Este es el relato y los descargos del ingeniero que creó el software que habría permitido extraer los supuestos mensajes de WhatsApp que involucraron a comuneros mapuches en atentados incendiarios".

Es indispensable indicar que, en dicha entrevista, Alex Smith ratifica ser el creador del programa y explica de forma teórica cómo funcionaba el software espía. Incluso se incorporan gráficas ilustrativas en el reportaje donde se informaba la metodología de operación, con envío de correo con la técnica de "phishing", es decir, con forma engañosa y fraudulenta, para efectos que la víctima del espionaje hiciera click en link incluido en dicho correo y así ser infectado por la aplicación que, luego de tomar control de las contraseñas del correo electrónico, podía interceptar comunicaciones privadas y reenviar la información a un servidor especial que, a través de un servicio web, podía revisar toda la información recopilada por medio de la aplicación, es decir, textos, conversaciones, imágenes y archivos adjuntos a mensajerías instantáneas.

Ahora bien, es determinante para los hechos fundantes de este recurso, que en dicha entrevista Alex Smith (a contar de los 7 minutos y 45 segundos del reportaje) señala literalmente que la FBI había visto el prototipo del programa **"porque como nos quitaron... a mi me allanaron todo, yo no quedé con nada... hasta las recetas familiares pensaron que eran código..."**. La situación a la que se refiere Alex Smith corresponde a las diligencias realizadas por Policía de Investigaciones por órdenes de la Fiscalía. Es así, como por la prensa[10] se informó que el día 26 de enero de 2018, la Brigada de Investigaciones Policiales Especiales (BIPE) de la Policía de Investigaciones (PDI) realizó el tercer allanamiento en el contexto de la querella de Fiscalía por las falsificaciones de pruebas de la "Operación Huracán". Se indicó que el procedimiento se llevó a cabo en una casa del radio urbano de Temuco, perteneciente al creador del software (Alex Smith). Según se lee en la nota, este allanamiento se transforma en el tercero realizado por PDI, luego de acceder a las instalaciones de Labocar y al cuartel de la Unidad de Inteligencia Operativa Especial (UIOE) de Carabineros en Temuco. Procedimiento que pudo avanzar después de varias horas, ya que la institución uniformada había solicitado 48 horas para hacer efectiva la entrega de equipos y documentación a la PDI.

[9] Video disponible para su visualización en http://www.t13.cl/videos/nacional/video-relato-del-acusado-montaje-operacion-huracan

[10] Noticia disponible en versión digital en http://www.soychile.cl/Temuco/Politica/2018/01/26/513531/PDI-realiza-allanamiento-a-domicilio-en-Temuco-correspondiente-a-creador-de-software-que-permitio-alterar-mensajes-de-wathsapp.aspx

En conclusión, Alex Smith ya no contaba ni con el software "antorcha" ni con el servidor al cual iban dirigidos los datos interceptados en equipos infectados por el programa espía.

Ante estos hechos antes descritos y las dudas que han surgido respecto a la existencia del programa espía "antorcha", las declaraciones de Alex Smith previamente han sido minuciosamente analizadas por diversas personas. Es así, como por ejemplo que frente a las precisiones técnicas que entregó Smith, éstas fueron criticadas por el ingeniero en redes y experto en seguridad, Paulo Colomés, quien elaboró un documento de 24 páginas[11] que publicó en la red social LinkedIn, donde fue derribando punto por punto, lo expuesto por el colaborador de la policía uniformada. Paulo Colomés termina concluyendo que "definitivamente Alex Smith Leay está mintiendo y su software ni siquiera es capaz de responder a un simple click".

Frente a estos cuestionamientos y ante la pregunta de Emilio Sutherland, respecto a ¿qué les respondería a esos tipos que tratan de "chanta" ?, Alex Smith respondió "... al final el chileno es chaquetero, me da lo mismo lo que opinan...".

Sin embargo, a continuación de sus dichos, en el reportaje se reveló otra información altamente preocupante para los que presentamos este recurso de protección. Así, ante la pregunta del periodista Emilio Sutherland **"¿pero le contó entonces en teoría...?** refiriéndose a una posible contradicción respecto a cómo demostraría el uso del programa si había sido incautados equipos, programas y códigos por parte de la PDI, a funcionarios de la FBI, Alex Smith respondió sin dudar "**No en teoría... porque habíamos desarrollado... estamos volviendo a desarrollarlo, pero ya está funcionando...".** Con esta declaración Alex Smith públicamente señala que está nuevamente creando el software "antorcha", a pesar de las medidas a las que fue objeto.

Acto seguido, continuando con la entrevista, el periodista le consulta nuevamente "... en la práctica le mostró a los agentes de la FBI..." y agregó... "y ellos pudieron ver cómo funcionaba". Ante ambas preguntas a cada una de ellas Alex Smith respondió **"sí"**.

Es este hecho ABSOLUTAMENTE pertinente como fundante de hecho de este recurso, toda vez que Alex Smith señala públicamente que está desarrollando nuevamente el mismo programa "antorcha", con el mismo objetivo y finalidad. Incluso se ratifica este hecho cuando se menciona que el mismo Alex Smith viajará en los próximos días a EE. UU. para trabajar directamente con los funcionarios de la FBI. Para ratificar lo anterior, Alex Smith claramente señala "**el objetivo es poner a prueba esta aplicación y yo voy a explicar técnicamente como se realiza esta intervención bajo un ministro de corte...**"

Con la sola emisión de este capítulo de reportaje y la entrevista en exclusiva otorgada por Alex Smith a Canal 13 podríamos inferir, casi sin equivocación, que con sus conocimientos técnicos el recurrido del presente recurso tiene condiciones para volver a desarrollar el programa "antorcha" aunque no cuente con su computador,

[11] El documento al que hacemos referencia se encuentra disponible en https://es.slideshare.net/pcolomes/observaciones-tecnicas-software-antorcha-operacin-huracn

equipos informáticos propios, posibles manuales de uso ni servidor donde interactuaba el programa espía, toda vez que están requisados por órdenes de Fiscalía.

Con este sólo hecho, sus declaraciones respecto a rol en "operación Huracán" y dichos concretos legítimamente podemos concluir que su habilidad para generar aplicaciones espías, llámense "antorcha" o cualquier otra denominación, pero que tienen el mismo único objetivo (el de afectar dispositivos móviles de terceros e intervenir comunicaciones privadas) es posible. De hecho, el mismo Alex Smith señala literalmente que la aplicación que desarrolló **interviene los equipos y las comunicaciones privadas**.

Sin perjuicio de lo anterior, nuestra mayor preocupación y conclusiones antes mencionadas se ratificaron completamente, cuando al terminar el capítulo de reportaje, el periodista Emilio Sutherland termina diciendo "**... hoy conocimos el testimonio del ingeniero Alex Smith, inventor de la llamada aplicación "antorcha" ... mañana pondremos a prueba su invento, es decir, en concreto, si se pueden ver imágenes y mensajes que se transmiten a través de WhatsApp o telegram...**"

Es así como el día siguiente, lunes 12 febrero recién pasado, se emite un segundo capítulo y final del reportaje exclusivo de Canal 13 transmitido en su señal abierta. Según se indica en el sitio web del canal donde es posible ver el capítulo[12], se lee lo siguiente: "Operación Huracán: El creador de "Antorcha" explica cómo funciona. Álex Smith puso a prueba el sistema que habría extraído los mensajes de WhatsApp y Telegram de los celulares incautados a los comuneros mapuche en el marco de la Operación Huracán."

Para nuestra mayúscula sorpresa y preocupación, el periodista Emilio Sutherland nuevamente se reúne con Alex Smith y es desafiado a someter a prueba el programa "antorcha". Ante la pregunta del periodista "Ud. está seguro de que nos va a demostrar que su aplicación es efectiva...", Alex Smith responde "es efectiva... sí".

En dicho reportaje el periodista señala que previamente a la prueba, se le entregó a Alex Smith, en forma voluntaria, "el número telefónico, el IMEI del aparato, y además los 2 correos electrónicos asociados a este teléfono. En concreto la idea es que este hombre demuestre ante las cámaras de Canal 13, la efectividad de su aplicación...". Posteriormente ante la insistencia respecto a qué les diría a esos peritos que lo tratan de chanta, Alex Smith señala "veremos quién es el chanta", con tono de seguridad y confianza en sus dichos respecto a las "bondades" y "efectividad" del programa "antorcha".

Es así como a contar de los 6 minutos del programa, llegan a la parte medular de la entrevista, en orden a demostrar empíricamente la **"intervención"**, palabra que es reafirmada por Alex Smith y que también él lo llama como **"infección"**. A continuación, se demuestra que al correo del periodista se le envió un email con una noticia referida a la búsqueda de la niña perdida (hasta ese entonces) de la sexta región llamada Emmelyn. Alex Smith explica que "depende del perfil del blanco a estudiar, se le envía una noticia, una oferta, un regalo, se le envía un diseño que sea interés de

[12] Video del capítulo disponible para su visualización en http://www.t13.cl/videos/nacional/video-operacion-huracan-creador-antorcha-explica-como-funciona

Ud.…". Ante eso Emilio Sutherland dice "o sea como yo soy periodista..." y Alex Smith responde "enviamos una noticia".

El objetivo de ese correo es que su receptor, el sujeto a intervenir en sus comunicaciones privadas, abra el correo enviado por el que utiliza el programa "antorcha". Una vez abierto, y sin saberlo, instala un programa espía que comienza a registrar el correo de la víctima y su contraseña. En el caso concreto del reportaje, Alex Smith frente a las cámaras le indica que "**ya tengo su clave, la Ip, de ud.**". Se refiere Alex Smith que frente a este envío de "phishing", es decir, simulación y engaño por medio de un mensaje, el simple acto se abrir el correo y revisar este mensaje, pudo obtener la contraseña del correo electrónico del tercero y con ello tiene el control de la casilla de email. Al mismo tiempo instala un "malware" o programa que se instala y que a través del mismo correo son despachados los mensajes de whatsapp y telegram a un servidor. Textualmente Alex Smith señala **"nosotros enviamos un "phishing y códigos dentro del correo... entonces necesitamos que el usuario lo abra, al abrirlo, nosotros optamos a varios caminos. Si él abre el "phishing", tenemos su clave. Si no, optamos a la... entramos a su sistema operativo, que puede demorar minutos o hasta horas..."**.

Para justificar y acreditar sus dichos, Alex Smith le menciona a Sutherland los datos de su email, contraseñas e ip del dispositivo y le señala que desde ese momento él puede entrar a su email desde ahí y revisar su correo electrónico y descargar información.

A continuación, en el reportaje se efectuaron conversaciones a través de mensajería instantánea WhatsApp entre el equipo "infectado" del periodista y otro diferente, que no tenía el programa espía instalado. La idea de producción era comprobar si era factible que Alex Smith, a través del programa "antorcha" pudiera rescatar estas u otras conversaciones. Es así como durante este proceso Alex Smith explica que está descargando la hora, la fecha, número de teléfonos conectados y se encontraba procesando las conversaciones. Señala al mismo tiempo que se va a descargar todas las fotos del teléfono y que la batería del mismo va a durar mucho menos por eso. En cuanto al tiempo de procesamiento, puede durar entre horas o días dependiendo de la cantidad de información procesada por la aplicación.

En el reportaje se muestra el término de la jornada de grabación y se comenta que, durante las pruebas, el sistema del servicio web del servidor donde se recopilaba la información supuestamente había sido "hackeado". Paradójicamente aparece en esta entrevista una abogada, la misma que representa a Alex Smith en la investigación de fiscalía por sabotaje informático, obstrucción a la investigación y falsificación de evidencias en el marco de la denominada Operación Huracán. En ella menciona que acá se cometería un delito informático por estos terceros por vulnerar un sistema de información y se afectaron los datos intervenidos en ella. Esto justificaría la demora en seguir obteniendo la información del equipo infectado del periodista.

Con posterioridad, se comienza a mostrar algunos resultados específicos con el uso del programa antorcha. Así, se identifica que en una conversación de WhatsApp se habría mandado una fotografía a una hora determinada lo que fue confirmado por el periodista. Además, confirma que ciertos caracteres, que Alex Smith denomina como "código fuente" de las conversaciones previo a su decodificación, corresponden a la misma cantidad de caracteres que tiene cada mensaje, en donde además se identifica la fecha y la hora de estos mensajes. Finalmente hace lectura de ciertas frases recopiladas

con el programa y al comparar con lo que efectivamente se había escrito, existían equivalencias parciales.

Nos llama la atención en esta parte de la entrevista que Alex Smith señalara que paralelamente a la prueba realizada con el equipo del periodista de Canal 13, también tenía infectado el equipo celular de su abogada, quien voluntariamente accedió a esto y "de otras personas" sin especificar a quienes se refería ni si habían manifestado su voluntad para estas pruebas. Esta abogada confirma abiertamente que los documentos que contaba Alex Smith en su computador, producto de la interceptación (tal como se señala literalmente) en su teléfono móvil, correspondía a los que originalmente se encontraban en su celular, documentos que esta misma abogada clasifica como secretos y que habrían sido enviados por WhatsApp.

Finalmente, la prueba termina cuando se exhibe que la conexión entre la aplicación espía que se encontraba en el celular y el servidor que recogía la información había sido cancelada por un firewall, que es un programa de seguridad. Sin embargo, las últimas declaraciones de Alex Smith señalan que "**desarrollamos esto en 4 días con pocos recursos que tenemos... si hubiéramos tenido más le hubiéramos sacado toda la información**". Con esta declaración, lo que Smith quiere señalar es que se demoró esa cantidad de tiempo para desarrollar nuevamente el programa "antorcha" y especialmente para hacer la prueba con el periodista de Canal 13, el cual termina concluyendo que a su entender "es un hecho concreto que sí se pueden interceptar mensajes de WhatsApp a través de estas aplicaciones".

A modo de resumen, luego de explicar con detalle todos los hechos que consideramos relevantes y fundantes para el presente recurso de protección, tenemos que:

- Sin perjuicio de solicitar se tenga por acreditados todos los hechos que sirven de sustento a favor de comuneros mapuches antes mencionados y que no queremos repetir nuevamente, se vuelve a confirmar que existe un reconocimiento expreso que Alex Guillermo Smith Leay desarrolló una aplicación que lo denominó "antorcha"y cuya propiedad intelectual es de este individuo, toda vez que la confeccionó personalmente y la facilitó a terceros (en este caso a Carabineros) a título gratuito para su uso para labores de investigación de la DIPOLCAR. No existe constancia de haber facilitado el programa a terceros, pero tampoco existe certeza de que no lo haya realizado.

- Con fundamentos ya no en trascendidos de prensa, sino directamente de sus propias declaraciones, Alex Smith reconoce que la PDI allanó su casa y le incautaron todos los dispositivos electrónicos, documentación, software y no quedó con ningún elemento del programa "antorcha" que utilizó para colaborar con Inteligencia de Carabineros.

- Confirmando este hecho, se acredita al mismo tiempo el hecho que Alex Smith en 4 días (según sus propias declaraciones) logró desarrollar nuevamente otra versión del software "antorcha", esta vez para mostrarlo públicamente y ser exhibido su funcionamiento y eficacia por el periodista de Canal 13, programa que fue ampliamente difundido. Tiene por tanto las competencias y capacidades para seguir

desarrollando el mismo programa o similares en cuanto a su objetivo, no importando el nombre del mismo.

- Debemos tener como hecho cierto, que el objetivo del programa continúa siendo interceptar comunicaciones privadas, intervenir equipos celulares y lograr acceder a las cuentas de correo con técnicas ilegales como "phishing" y "malware".

- Queda acreditado que con estas herramientas cualquier persona puede ser objeto de ser considerado un "blanco" o afectado por el programa "antorcha", porque la elección de la víctima es seleccionado por el operador del software en forma arbitraria.

- Se acredita al menos que con la infectación del equipo celular se tuvo acceso a cuenta de correo electrónica, donde se pudo determinar la casilla de email y su contraseña, y por otro lado, que pudo parcialmente obtener datos de conversaciones de mensajería instantánea y documentos e imágenes enviados a través de estas mensajerías potencialmente explotadas, como son whatsapp, telegram y facebook messenger.

- Al igual que los comuneros mapuches a nombre de los cuales presentamos este recurso, los firmantes de este recurso tuvimos conocimiento público el día viernes 09 de febrero recién pasado, cuando el Juez de Garantía de Temuco acogió la petición de la Fiscalía para cerrar la investigación y su decisión de no perseverar en la investigación en el marco de la "operación Huracán", de la existencia de este programa "antorcha", de sus funciones, características y posibilidades de uso en contra de cualquier persona. Sin perjuicio de ello, por declaraciones del mismo Alex Smith en los 2 capítulos de reportajes de Canal 13, transmitidos este día 11 y 12 de febrero recién pasado, logramos obtener la convicción de que este ingeniero podía desarrollar nuevamente "desde cero" el programa "antorcha" o cualquier otro con el mismo objetivo, independiente sea el nombre, que tiene las competencias para ésto y que además este tipo de programas tienen por finalidad exclusivamente la interceptación de las comunicaciones privadas, siendo cualquier persona potencial víctima del software creado.

- También se acredita que este software puede ser utilizado en cualquier oportunidad, espacio de tiempo, motivo o razón, tal como lo realizó en las pruebas grabadas y exhibidas en televisión, sin que sea exclusivamente utilizado para labores de investigación o por personal de inteligencia de Carabineros al amparo de la Ley de Inteligencia del Estado. En conclusión, el poseedor material del software lo puede utilizar arbitrariamente, contra cualquier persona, por cualquier motivo o circunstancia, lo que acredita por tanto nuestro legítimo temor y amenaza en nuestros derechos constitucionales que posteriormente desarrollaremos en el presente escrito.

EL DERECHO:

Es absolutamente relevante mencionar que la Constitución Política de Chile establece la facultad de presentar ante órgano juridiccional diversos recursos, siendo uno de ellos el recurso de Protección. El objetivo de un recurso de protección es

restablecer el derecho y dar protección al afectado cuando, por causa de actos u omisiones arbitrarias o ilegales, cometidos por cualquier persona o autoridad sufra la privación, perturbación o amenaza en el legítimo ejercicio de ciertos derechos y garantías específicamente establecidos en la Constitución.

Debemos aclarar en primer lugar que el presente recurso de protección, presentados en nombre y a favor de los comuneros mapuches, por un lado, y respecto de los cuales a nuestro entender se han visto afectados directamente por actos ilegales y arbitrarios, no va dirigido ni contra Carabineros de Chile, Ministerio Público ni contra Intendencia de Temuco, quienes son querellantes en la causa investigada denominada "Operación Huracán". Tampoco nos hacemos cargo del proceso de investigación y posibles irregularidades que han surgido por manipulación de pruebas presentadas y que actualmente se encuentran en etapa de investigación.

Esta acción constitucional está dirigida en contra del autor - desarrollador del programa "antorcha", el cual fue creado y utilizado, tal como consta en los hechos, en el marco de la investigación a la que estuvieron sometidos los comuneros mapuches, con la finalidad de interceptar sus comunicaciones privadas y acceder a información de sus respectivos dispositivos móviles y que puede a su vez ser utilizado en el futuro contra cualquier persona, en cualquier circunstancia, incluso cuando exista investigaciones judiciales en su contra.

Es relevante señalar que, como obra de la propiedad intelectual, el software está protegido bajo las leyes de derechos de autor. Así, nuestra legislación la reconoce a nivel constitucional y legal.

La Constitución Política de 1980, en su artículo 19, Nº 24, establece "el derecho de propiedad en sus diversas especies sobre toda clase de bienes corporales e incorporales"; más particularmente en el artículo 19 Nº 25, señala "el derecho del autor sobre sus creaciones intelectuales y artísticas de cualquier especie, por el tiempo que señale la ley y que no será inferior al de la vida del titular".

De estos dos artículos emana la normativa legal vigente relativa a los derechos sobre el Software.

Por otro lado, el Código Civil establece en el artículo 584 que "las producciones del talento o del ingenio son una propiedad de sus autores. Esta especie de propiedad se regirá por leyes especiales".

La ley Nº 17.336 contempla todo lo referente a la Propiedad Intelectual, y en su artículo Nº 3 establece que "quedan especialmente protegidos los programas computacionales". Además el artículo Nº 1 de dicha ley señala a la letra: "La presente Ley protege los derechos que, por el solo hecho de la creación de la obra, adquieren los autores de obras de inteligencia en los dominios literarios, artísticos y científicos, cualquiera que sea su forma de expresión, y los derechos conexos que ella determina".

Ahora bien, ¿Qué se entiende por programa computacional?

Se define como programa computacional: "un conjunto de instrucciones para ser usadas directa o indirectamente en un computador a fin de efectuar u obtener determinado proceso o resultado, contenidas en un diskette, cassette, cinta magnética u otro soporte material".

Además se establece que se entenderá por "conjunto de instrucciones" que constituye el programa computacional un grupo de instrucciones ya sea bajo la forma de "Programa Fuente" o de "Programa Objeto".

Por tanto, la posible mención de Alex Smith respecto a que el programa “antorcha” sea una aplicación y no un software no tiene sustento legal, porque son normativamente lo mismo.

Con estas consideraciones de derecho y a la luz de los antecedentes de hecho, queda claro que el autor de la aplicación llamada “antorcha”, que en definitiva es un software, y, sobre el cual se generan sus respectivos derechos de autor (y por consiguiente las obligaciones respectivas), corresponden a Alex Smith Leay, quien demostró incluso posteriormente al cierre de la investigación de la Operación Huracán, y especialmente para programa de reportaje de Canal 13, desarrollando nuevamente la aplicación, que es el autor del mismo.

Es importante indicar que en términos generales se reconoce que los derechos de autor son patrimoniales y morales, es decir, son derechos relacionados con el aprovechamiento, paternidad e integridad de la obra.

Algunos derechos morales son: reivindicar la paternidad de la obra, asociándole el nombre o seudónimo del autor; oponerse a toda modificación sin su consentimiento; mantener la obra inédita, y autorizar a terceros a terminar una obra inconclusa. En este caso concreto el derecho moral le corresponde exclusivamente a Alex Smith, toda vez que desarrolló la aplicación directamente por él. Al mismo tiempo queda acreditado que le realizó sucesivas mejoras en distintas versiones, por lo que ratifica este hecho.

Por otro lado algunos derechos patrimoniales son: publicación de la obra, adaptación de la misma a otro género, reproducción por cualquier procedimiento y distribución mediante venta. En este caso no existe constancia que haya transferido sus derechos patrimoniales de autor a persona o institución alguna, no existiendo constancia de alguna compraventa o cesión de ninguna especie. Sólo existe el hecho que facilitó para ser usado en diversas investigaciones a Carabineros de Chile. El hecho de haber sido contratado como asesor informático de Carabineros tampoco acredita el hecho que haya celebrado algun acto de cesión de derechos patrimoniales a ésta institución

Considerando, por tanto, todos estos antecedentes, queda de manifiesto que el autor, responsable del programa, de sus funciones, facultades y objetivos de uso le corresponden específicamente a Alex Smith.

Se encuentra completamente acreditado que el objetivo del programa “antorcha” (y conforme a la definición de programa informático) fue diseñar un conjunto de instrucciones para ser usadas directamente sobre un sistema operativo de un dispositivo móvil a fin de efectuar u obtener determinado proceso o resultado, que consistía en interceptar comunicaciones privadas, tomar control de cuentas de correo y acceder a información privada tales como comunicaciones de mensajería instantánea como whatsapp, telegram y facebook messenger, sin la autorización previa, informada y conciente de víctimas (o blancos como denominó Smith), vulnerando sus sistemas y violando sus derechos constitucionales. No existe otro fin diverso para este programa porque no tiene ninguna lógica el desarrollo de este programa para acceder con consentimiento de los afectados, toda vez que tal como señala, utilizaba técnicas de

envío de correo con “phishing” e insertando código malware, con clara infracción de la ley. Es posible concluir que su utilización es posible de realizar en cualquier momento, contra cualquier persona, en cualquier circunstancia, ya sea para obtener información en forma particular, para defraudar a un tercero, para obtener secretos mercantiles o comerciales si el objetivo es una empresa privada, obtención de información secreta o clasificada, ser utilizado para estafa, y así un múltiple etcétera de posibilidades de uso y motivos para su utilización y siendo finalmente cualquier persona, institución pública o privada, objeto de vulneración de sus comunicaciones privadas, por lo que, quienes presentamos este recurso a nombre propio, detentamos actualmente la situación de posibles víctimas y objetivos de uso de este programa espía.

Es así como el fundamento legal que encontramos en el derecho de creación de aplicaciones, software y programas informáticos no tiene ninguna limitación más que prohibiciones legales.

Es importante destacar por tanto, que existe libertad para crear programas informáticos, sin embargo si el software tiene como finalidad exclusiva, determinante y su desarrollo busca lesionar derechos y garantías constitucionales es abiertamente ilegal.

En el caso en comento, existe una prohibición indicada a nivel constitucional y que corresponde a lo establecido en el artículo 19 N° 5 respecto a que la Constitución Política asegura la inviolabilidad del hogar y de toda forma de comunicación privada. El hogar sólo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley.

Es decir, Alex Smith, al diseñar, crear, replicar y mejorar el programa “antorcha” y cuyo objetivo es interceptar comunicaciones privadas y al mismo tiempo acceder a estas comunicaciones y documentos privados, tal como se indica en la garantía constitucional, actúa ilegalmente y dicho software en consecuencia es ilegal.

Respecto a éste último punto, se establece que sólo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley.

Debemos buscar, por tanto, en la legislación chilena, las consideraciones de derecho respecto de cuales son los casos excepcionales en que la ley determine, las circunstancias y formas que autoricen expresamente el que las comunicaciones y documentos privados puedan interceptarse, abrirse o registrarse.

1) Norma del Código Procesal Penal:

a. El artículo 222 y siguientes del Código Procesal Penal establece los casos y formas en que las comunicaciones pueden interceptarse, abrirse o registrarse, de forma excepcional y en cumplimiento a la reserva de ley establecida en el numeral 5 del artículo 19 de la Constitución.

b. Casos en que procede la interceptación: solo podrá interceptarse una comunicación telefónica cumpliendo los siguientes requisitos:

• Si existieren fundadas sospechas, basadas en hechos determinados de la relación de una persona con el hecho punible que merezca pena de crimen: ha cometido el crimen; ha participado en la preparación o comisión del crimen; ha preparado la comisión o participación del crimen. En este apartado no se incluyen los

actos preparatorios, los cuales son punibles solo excepcionalmente, conforme a lo dispuesto en el artículo 8° del Código Penal.

• Si la investigación lo hiciera imprescindible. En este caso, el Juez de Garantía, a petición del Ministerio Público, podrá ordenar la interceptación y grabación de comunicaciones telefónicas o de otras formas de telecomunicación. Dicha orden solo podrá afectar al imputado o a personas respecto de las cuales existieren sospechas fundadas, basadas en hechos determinados, de que sirven de intermediarias de dichas comunicaciones y, asimismo, de aquellas que facilitaren sus medios de comunicación al imputado o sus intermediarios.

c. Requisitos que debe contener la orden de interceptación y grabación: la orden del Juez de Garantía, a solicitud del Ministerio Público, deberá indicar circunstanciadamente: nombre y dirección del afectado por la medida; forma de interceptación de la comunicación; plazo, que no podrá exceder sesenta días. El plazo es prorrogable por períodos de igual duración, para lo cual el juez deberá examinar cada vez la concurrencia de los requisitos para la intercepción. Cumplido el plazo fijado o disipadas las sospechas, la medida deberá ser interrumpida inmediatamente.

d. Comunicaciones que no pueden ser interceptadas: no pueden ser interceptadas las comunicaciones entre el imputado y su abogado, a menos que el Juez de Garantía lo ordenare, por estimar fundadamente que el abogado pudiere tener responsabilidad penal en los hechos investigados.

e. Rol de las empresas telefónicas y de comunicaciones: las empresas telefónicas y de comunicaciones deberán llevar a cabo las medidas ordenadas por el Juez de Garantía, proporcionando a los encargados las facilidades para el oportuno cumplimiento de estas, sin negativas ni entorpecimientos, los cuales serán constitutivos de desacato.

Además deberán guardar secreto acerca de las mismas, salvo que sean citadas como testigos. Como medida previa, dichas empresas deberán mantener un listado actualizado de sus rangos autorizados de direcciones IP y un registro de los números IP de las conexiones que realicen sus abonados, no inferior a un año.

f. Registro de la interceptación y destrucción de copias: la interceptación telefónica será registrada mediante grabación magnetofónica u otros medios técnicos análogos que aseguraren la fidelidad del registro. Debe ser mantenido bajo sello, custodia y conservación de los originales por parte del Ministerio Público, a quien será entregada de forma directa. El Ministerio Público podrá disponer la transcripción escrita de la grabación por un funcionario, quien actuará como ministro de fe para efectos de su fidelidad.

g. La incorporación al juicio oral de los resultados se realizará de la manera que determine el tribunal en la oportunidad procesal respectiva, reservándose la facultad de citar como testigos a los encargados de practicar la diligencia. Las comunicaciones irrelevantes serán entregadas a las personas afectadas con la medida y se destruirá toda transcripción o copia de ellas por el Ministerio Público, a menos que contengan informaciones relevantes para otros procedimientos sobre delitos que merezcan pena de crimen.

h. Notificación al afectado: la medida intrusiva será notificada al afectado con posterioridad a su realización, si la investigación lo permitiere y si no pusiere en peligro la vida o integridad corporal de terceras personas. En caso contrario regirá lo dispuesto en el artículo 182 del Código Procesal Penal, que regula el secreto de las actuaciones de investigación.

i. Prohibición de utilización de los resultados de la medida: no podrán ser usados los resultados de la interceptación telefónica cuando ella hubiere tenido lugar fuera de

los supuestos previstos por la ley o incumpliendo los requisitos de los artículos 222 y siguientes, sobre interceptación de comunicaciones telefónicas, a que se hizo referencia anteriormente.

Es relevante mencionar que Alex Smith no forma parte del Ministerio Público, ni es funcionario de empresa de telecomunicaciones y por tanto al crear y desarrollar el software "antorcha" no lo hizo con la finalidad de cumplir con el artículo 222 del Código Procesal Penal. Incluso las funcionalidades del software exceden ampliamente los casos y formas establecidas en dicha ley, toda vez que este artículo en comento habla de interceptación telefónica, es decir, estamos hablando de voz que se transmite por medios analógicos o digitales de comunicaciones y en cuyo caso se permite su interceptación y grabación de conversaciones. En el caso del programa "antorcha" su funcionalidad no es interceptar comunicaciones telefónicas sino que interceptación de comunicaciones digital, es decir, datos, los cuales eran transmitidos desde los equipos celulares "infectados" hasta un servidor web, a través de internet, que tenía por finalidad almacenar la información privada "recuperada" por medio de la aplicación.

A todas luces, por tanto, Alex Smith no estaría actuando, con la creación y desarrollo del software "antorcha" ajustándose a esta normativa legal, lo que nos hace ratificar la ilegalidad de su creación intelectual.

2) Norma de Ley 19.974 Sobre el Sistema de Inteligencia de Estado

En este punto, específicamente para el caso de los comuneros mapuches, DIPOLCAR invocó la Ley de Inteligencia del Estado, Ley 19.974, en virtud del cual, en su artículo 23 inciso 1° y 2° reza:

Artículo 23.- Cuando determinada información sea estrictamente indispensable para el cumplimiento de los objetivos del Sistema y no pueda ser obtenida de fuentes abiertas, se podrá utilizar los procedimientos especiales de obtención de información a que se refiere el presente Título, en la forma y con las autorizaciones que en el mismo se disponen.

Dichos procedimientos estarán limitados exclusivamente a actividades de inteligencia y contrainteligencia que tengan por objetivo resguardar la seguridad nacional y proteger a Chile y su pueblo de las amenazas del terrorismo, el crimen organizado y el narcotráfico.

Esto quiere decir que sólo en determinados casos muy, pero muy excepcionales, Carabineros en forma autónoma puede investigar. En esta causa se justificó la investigación contra comuneros mapuches que son los que coincidentemente se presenta a su favor el presente recurso de protección, bajo la denominación de "delitos terroristas". No contentos con ello, DIPOLCAR utilizó los llamados "procedimientos especiales" para la obtención de las pruebas presentadas.

Artículo 24.- Para los efectos de esta ley se entiende por procedimientos especiales de obtención de información, los que permiten el acceso a antecedentes relevantes contenidos en fuentes cerradas o que provienen de ellas, que aporten antecedentes necesarios al cumplimiento de la misión específica de cada organismo operativo.

Tales procedimientos son los siguientes:

a) La intervención de las comunicaciones telefónicas, informáticas, radiales y de la correspondencia en cualquiera de sus formas;

b) La intervención de sistemas y redes informáticos;

c) La escucha y grabación electrónica incluyendo la audiovisual, y

d) La intervención de cualesquiera otros sistemas tecnológicos destinados a la transmisión, almacenamiento o procesamiento de comunicaciones o información.

Para poder utilizar estos procedimientos especiales la Ley indica que previamente deben ser autorizados por un Ministro de Corte de Apelaciones en cuya jurisdicción ocurriera los hechos investigados.

Este punto es el determinante en derecho. Por un lado consta en los hechos y declaraciones que el software "antorcha" fue desarrollado por Alex Smith con anterioridad a la solicitud de procedimientos especiales por parte de Inteligencia de Carabineros y que este software fue implantado con anterioridad a esta autorización (toda vez que existe incluso presuntos registros de conversaciones con anterioridad a la autorización del Ministro de Corte de Apelaciones de Temuco),

Consta al mismo tiempo que lograda la autorización por parte del Ministro de Corte de Apelaciones, Inteligencia de Carabineros utilizó el software "antorcha" de propiedad de Alex Smith , y que consideramos ilegal en cuanto a los objetivos de su creación, en perjuicio de los comuneros mapuches y con autorización de uso expresa del creador del software. Es decir, teniendo conocimiento de que este software tenía una finalidad contraria a la ley (de interceptar comunicaciones privadas), Alex Smith autorizó su uso justamente para este fin de investigación.

Paralelamente existe la dicotomía respecto a que Inteligencia de Carabineros, obteniendo la autorización de ministro de corte de apelaciones de Temuco, podía intervenir las comunicaciones telefónicas, informáticas, sistemas y redes informáticas, intervenir cualquier otro sistema tecnológico destinado a la transmisión, almacenamiento o procesamiento de comunicaciones o información, pero de NINGUNA MANERA la ley permite que sea realizado utilizando un software o programa informático que desde su génesis tiene como objetivo infringir abiertamente la ley y garantía constitucional de inviolabilidad de las comunicaciones privadas.

Podríamos tener una interpretación amplia respecto a que Inteligencia de Carabineros podría utilizar tecnología sólo para fines de investigación invocando la ley de Inteligencia del Estado, si esta institución sea la que previamente desarrollara para sí (y por tanto ser la creadora del software y titular de derechos de autor) y nunca utilizarlo para ningún otro uso, cesión u objetivo diferente, que para cuando tuvieran la autorización de Ministro de Corte de Apelaciones en investigaciones específicas. Sin embargo, creemos a todas luces, que esta interpretación amplia también es cuestionable.

Por otro lado, en caso de que existiera autorización previa a funcionarios de inteligencia, toda medida debe cumplirse y orientarse con el principio de finalidad de la acción. Así, utilizar, a nuestro modo de entender, acciones de intervención de comunicaciones por vía de malware, técnicas de phishing, envío de virus o troyanos y acciones similares, podría configurarse como excesivo y lesivo a la privacidad del investigado, que recordémoslo, aún no es acusado formalmente de un delito.

Como se debe concluir, sólo se encuentra facultado Inteligencia de Carabineros a utilizar únicamente medios legales (y no ilegales) propios para poner en práctica alguna de los procedimientos especiales establecidos en esta ley excepcional.

Para dar más contenido a esta discusión legal, es de vital importancia recordar que Alex Smith participó en investigaciones de DIPOLCAR y facilitó el software "antorcha", siendo un simple civil, no uniformado y sin ningún vínculo laboral con la institución, de manera no remunerada.

Podríamos aplicar acá perfectamente un inciso de la Ley de Inteligencia que menciona que "los que sin ser parte del Sistema de Inteligencia del Estado utilicen tales procedimientos, serán castigados con presidio menor en cualquiera de sus grados, sin perjuicio de las penas que correspondan por los crímenes o simples delitos cometidos con ocasión de la actividad ilícita". Podríamos entender por tanto que Alex Smith podría ser sancionado por esta norma adicional si se considera que no es parte de Sistema de Inteligencia desde antes de ser contratado (lo cual ocurrió en octubre de 2017) o si consideramos que ser contratado como ingeniero forestal no basta para ser considerado dentro del sistema de inteligencia del Estado.

Sin embargo éste no es un punto legal cuyas consecuencias nos compete, ni cómo funcionarios de Inteligencia llevaron a cabo sus atribuciones legal, sin embargo sí es relevante el hecho que utilizó y facilitó un software completamente ilegal para infectar a los comuneros mapuches a favor de los cuales se presenta el recurso (con anterioridad a autorización de Ministro de Corte de Apelaciones de Temuco) y por consiguientes cuyos derechos constitucionales fueron violados,

Por otro lado es el propio Alex Smith, que nos demuestra que la creación y desarrollo del software "antorcha" no encuentra su fundamento legal en la ley 19.974, toda vez que a pesar de que no cuenta con el software "antorcha" original (que fue requisado por órdenes de Fiscalía en la investigación por alteración de pruebas en el caso "Operación Huracán"), logró volver a crear el software en cuestión, fuera de una labor de inteligencia e investigación de la referida ley.

Es importante resaltar que con este hecho, actualmente cualquier persona, incluyendo a los firmantes de este recurso, somos posibles víctimas de la utilización de este software espía en nuestra contra, lo que abiertamente amenaza nuestro derecho constitucional de inviolabilidad de comunicaciones privadas.

Lo anterior queda absolutamente demostrado por el mismo Smith, quien utilizó el programa "antorcha", fuera de un proceso de investigación de inteligencia de Carabineros, amparados en la Ley 19,974. En este caso concreto demostró las capacidades y eficiencia de interceptación de comunicaciones para periodistas de Canal 13. Y a pesar que los equipos celulares infectados por el programa correspondían a personas que voluntariamente aceptaron esto, nada impide que pueda infectar equipos celulares de cualquier persona sin contar debida y previamente con su autorización.

3) Ley 20.000: Sobre Tráfico de Estupefacientes.

En la ley indicada existe una referencia a facultad que la ley otorga al Ministerio Público para que pueda interceptar comunicaciones privada.

Así el inciso primero del artículo 24° indica:

"Las medidas de retención e incautación de correspondencia, obtención de copias de comunicaciones o transmisiones, interceptación de comunicaciones telefónicas y uso de otros medios técnicos de investigación, se podrán aplicar respecto de todos los delitos previstos en esta ley y cualquiera sea la pena que merecieren, de conformidad a las disposiciones pertinentes del Código Procesal Penal."

Sólo volveremos a mencionar que Alex Smith no es funcionario de Fiscalía, no creó ni desarrolló el software a petición del Ministerio Público y por tanto, su creación intelectual no se ajusta a la norma legal analizada.

4) Decreto Ley 211: Fija Normas Para la Defensa de la Libre Competencia.

A la luz de esta normativa nos encontramos con una situación muy similar a la fijada por la Ley 19,974. En ella se indica, en lo medular y atingente a lo discutivo en autos, en su artículo 39°, otorga al Fiscal Nacional Económico, que en casos graves y calificados de investigaciones destinadas a acreditar conductas de las descritas en la letra a) del artículo 3°, solicitar, mediante petición fundada y con la aprobación previa del Tribunal de Defensa de la Libre Competencia, autorización al Ministro de la Corte de Apelaciones de Santiago que corresponda de acuerdo al turno, para que Carabineros o la Policía de Investigaciones, bajo la dirección del funcionario de la Fiscalía Nacional Económica que indique la solicitud, proceda a:

n.1) Entrar a recintos públicos o privados y, si fuere necesario, a allanar y descerrajar;
n.2) Registrar e incautar toda clase de objetos y documentos que permitan acreditar la existencia de la infracción;
n.3) Autorizar la interceptación de toda clase de comunicaciones, y
n.4) Ordenar a cualquier empresa que preste servicios de comunicaciones, que facilite copias y registros de las comunicaciones transmitidas o recibidas por ella.

Es relevante, por tanto recalcar, que la conducta de Alex Smith, quien no es el Fiscal Nacional Económico, al crear y desarrollar el software "antorcha", es contrario a derecho, porque tampoco destinó exclusivamente su creación intelectual para la investigación de interceptar comunicaciones a la luz del Decreto Ley 211.

Ratificamos que este Decreto Ley 211 tampoco autoriza para que por medios ilegales cumplir función investigativa, si es que se hubiera dado el caso que haya encomendado la gestión de desarrollo del software exclusivamente para estos fines a Alex Smith, lo que no ocurrió en los hechos.

Finalmente indicamos que NO EXISTE ninguna otra norma legal que justifique o ampare el que las comunicaciones y documentos privados puedan interceptarse, abrirse o registrarse.

Podemos por tanto concluir que en el ejercicio de crear y desarrollar software, al crear, diseñar y realizar mejoras al programa "antorcha" por parte de Alex Smith, destinada a la interceptación de las comunicaciones en todas sus formas cometió una ABIERTA ILEGALIDAD y DEBE por tanto, ser considerado el software "antorcha" y

cualquier otro software con similares características, finalidades y objetivos, no importando su denominación o nombre de fantasía, como ILEGAL y no ajustado a derecho.

1. ACTO IMPUGNADO

Concretamente los actos impugnados son:

A) Creación de software "antorcha" cuyo objetivo, funcionalidad y capacidad es abiertamente ilegal.

B) Respecto a los comuneros mapuches a favor de los cuales se presenta el recurso de protección, el acto impugnado es que utilizó el software espía directamente sobre ellos, infectando sus equipos celulares, cuentas de correo, interceptación de sus comunicaciones de mensajería instantánea tales como whatsapp, telegram y facebook messenger, programa que se mantiene funcionando actualmente.

C) Respecto a los firmantes del presente recurso que nos presentamos a nombre propio, el desarrollo de un nuevo software, de iguales condiciones del original programa "antorcha", y el establecimiento de un nuevo servidor web para recopilar información interceptada, con posterioridad a la incautación del programa original, equipos, documentación y similares, por parte de Fiscalía; programa que actualmente puede ser utilizada en nuestra contra y ser considerados caprichosa y en forma arbitraria como "sujetos blancos" por parte de Alex Smith.

2. INDIVIDUALIZACION DE LA AUTORIDAD O PERSONA RECURRIDA

El acto ilegal y arbitrario ha sido cometido, generado o -para utilizar los términos del constituyente- es imputable a ALEX GUILLERMO SMITH LEAY.

3. ILEGALIDAD POR ACTOS

Tal como se desprende de todo lo señalado con anterioridad, la ilegalidad se establece completamente puesto que por un lado se reconoce constitucional y legalmente la posibilidad de creación y desarrollo de un software (surgiendo con ello su derecho de autor), pero encontrando como limitación una prohibición legal. Es así como se garantiza la inviolabilidad de las comunicaciones privadas y se fija a ésta como límite. Por su parte, Alex Smith, sin tener ningún fundamento legal habilitante, y consiente de que su ingenio afectaría precisamente derechos fundamentales garantizados en la Constitución, crea y desarrolla en diversas oportunidades el software "antorcha", que tiene como única y exclusiva finalidad la interceptación de las comunicaciones privadas.

Es tal su responsabilidad en este acto de creación, que posteriormente utiliza en múltiples oportunidades demostraciones a terceros de las "bondades" de su funcionalidad (ya sea a funcionarios de carabineros, fiscal de Rancagua, periodista de canal 13, su propia abogada), respecto de los cuales existe constancia y en los que en esas oportunidades autorizaron expresamente la infectación de sus equipos. Sin

embargo existe plena constancia, la cual se desprende de sus propias declaraciones, que también utilizó el software espía, sobre múltiples objetivos y en numerosas oportunidades, algunas fallidas y que lo convencieron en mejorar al menos en cuatro oportunidades, las características y eficiencia del software. No tenemos identificadas a las víctimas, pero existen, según él mismo ha mencionado, sobre todo cuando facilitó y manipuló su software en dependencias de DIPOLCAR y en procesos de investigación.

No obstante lo anterior, y tal como se consignó previamente, a pesar de no contar con el software "antorcha" original (producto de la medida de incautación que operó en su contra), volvió a crear, según él en sólo cuatro días, una nueva versión del software y utilización de servidor web, con las mismas características, funcionalidades y objetivo ilegal, lo que vuelve a demostrar su permamente actuar contrario y desafiante ante la ley.

4. ARBITRARIEDAD POR ACTOS

El ingeniero Alex Smith ha demostrado, dicho y creado el software "antorcha", el cual consideramos abiertamente ilegal, para ser utilizado ante cualquier persona, institución, pública o privada y sin hacer ninguna distinción.

Es así como de forma arbitraria decide hacer pruebas en múltiples objetivos, sin patrón común, realizando mejorar y dejando el software con la capacidad de utilizarlo en cualquier momento y en contra de quien estime arbitraria y caprichosamente. No existe ningún mandato, orden o atribución que identifique a las potenciales víctimas de su interceptación en comunicaciones privadas. Es tan así que decidió voluntariamente y sin ser contratado con Carabineros en participar en labores de investigación. Con esta misma idea de querer recabar información en forma ilegal decide aplicar el software sobre los comuneros mapuches a favor de los cuales se presenta este recurso, incluso antes de que carabineros invocaran la ley de Inteligencia del Estado. Adicionalmente y sin que exista orden legal emitida, ya decidió mostrar el programa espía fuera del país, tal como lo ha anunciado, específicamente a funcionarios de FBI de EEUU. Incluso, arbitrariamente decide mostrar su funcionalidad ante las cámaras de todo Chile, con equipos móviles de periodistas de Canal 13, ufanándose de la eficiencia de su creación en forma flagrante, a pesar que su software original se encontraba requisado por la justicia.

5. VIOLACIÓN DE DERECHOS AMPARADOS POR EL RECURSO DE PROTECCION.

Los derechos que asegura a todas las personas la Constitución Política de la República y que estarían claramente infringidos específicamente son (y tal como se anunció con anterioridad):

A) Artículo 19 nº 5, La inviolabilidad del hogar y de toda forma de comunicación privada.

La constitución asegura que el hogar sólo puede allanarse y específicamente menciona que las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley.

1) Con respecto a los derechos y garantías constitucionales de los comuneros mapuches a favor de los cuales se presenta el recurso de protección:

En el presente caso, Alex Smith al momento de crear el software "antorcha", claramente ilegal, y al infectar los equipos móviles de estos comuneros de manera concreta y dirigida, sin que esta conducta sea de los casos y en la forma determinada por la ley (porque incluso realizó tales acciones antes de que DIPOLCAR fuera autorizado al invocar la Ley de Inteligencia, y él sin ser funcionario de esta unidad de inteligencia), afectó de manera directa y flagrante este derecho a la inviolabilidad de toda forma de comunicación privada que la Constitución Política garantiza, teniendo como fundamentos los antecedentes de hecho y de derecho previamente señalados.

Volvemos a recordar que esta violación directa de sus derechos la realizó porque "infectó" sus equipos celulares, mediante la técnica de "phishing" (es decir mediante engaño y manipulación de información falsa) e implantación de "malware", lo que hizo que tomara control de estos dispositivos, de cuentas de correo, tuviera acceso a comunicaciones privada como son comunicaciones de aplicaciones de mensajería instantánea y accediendo a información confidencial y privada sin contar con la autorización de estos comuneros.

En los hechos, los equipos celulares de los comuneros, que se encuentran actualmente siendo periciados y con orden de comiso vigente, mantienen en su interior "infectados" por el software "antorcha" y se encuentra el servidor web operativo que recepcionaba información y comunicaciones privadas funcionando, por lo que sus derechos y garantías constitucionales actualmente siguen siendo violentados flarantemente. No ha sido eliminado el programa ni el servidor web inhabilitado.

Por este motivo, claramente creemos que como consecuencia de los actos arbitrarios e ilegales cometidas por Alex Smith, dichos comuneros sufrieron y se mantiene la privación y perturbación de sus derechos y garantías constitucionales indicada.

2) Con respecto a los derechos y garantías constitucionales respecto de quienes presentamos el recurso de protección a nombre propio y respecto de cualquier otro habitante de Chile:

Sin perjuicio de que, hasta este momento, no tenemos conocimiento de que Alex Smith nos haya considerado como "objetivos" o "blancos" para efectos de infectar nuestros teléfonos móviles, la Constitución claramente señala que también existirá tutela constitucional cuando como consecuencia de actos arbitrarios o ilegales, se sufren amenaza a derechos y garantías constitucionales.

Específicamente en nuestro caso, a la luz de los antecentes, ya el hecho de crear y desarrollar este software ilegal por parte de Alex Smith, y que podría ser utilizar en nuestra contra, nos genera una amenaza sobre nuestros derechos, sobre todo que depende exclusivamente de la arbitrariedad del autor del programa para ser blanco de esta aplicación.

Con posterioridad, a la luz de los antecedentes, respecto a orden de incautación de sofware "antorcha" original, de su documentación, equipamiento, servidores web, conforme a investigación realizada por Fiscalía por posibles delitos de manipulación de prueba en virtud de la "operación Huracán", podríamos decir que esta amenaza sobre nuestros derechos y garantías constitucionales fue atenuada por acción indirecta de la justicia, toda vez que esta medida es momentanea y nada dice respecto al posterior uso del programa una vez llevada a acabo la investigación por parte del Ministerio Público.

Sin embargo, con la exhibición pública del reportaje de Canal 13 y la declaración explícita de Alex Smith respecto a que a pesar de no contar con ningún elemento luego de la incautación antes mencionada, en sólo 4 días logró volver a desarrollar una aplicación con la misma denominación de software "antorcha" y que tiene las misma génesis en cuanto a ilegalidad y facultad de "infectar" e "interceptar" cualquier comunicación privada. Al mismo tiempo, demostró que mantiene operativo un servidor web distinto al allanado operativo y que tiene por finalidad recibir la información en forma ilegal.

Surge por estos antecedentes nuevamente una amenaza directa sobre nuestros derechos y garantías constitucionales, toda vez que existe la facilidad y arbitrariedad por parte de Alex Smith de considerarnos "blancos" de su programa y así "infectar" e "interceptar" nuestros equipos móviles sin fundamento legal, por lo que de estar actualmente amenazados en nuestros derechos y garantías constitucionales, con sólo su voluntad pasaríamos a ser sujetos de violación directa y flagrante de nuestos derechos y garantías constitucionales. Tal situación de amenaza de derechos y garantías constitucionales al mismo tiempo opera respecto a cualquier habitante de Chile, sin distinción.

B) Artículo 19 nº 4. El respeto y protección a la vida privada y a la honra de la persona y su familia.

Es importante comenzar diciendo que en Chile existe abundante literatura sobre el derecho a la vida privada, que intenta precisar en qué consiste este derecho: es entendido como intimidad, en el sentido de conciencia; como el derecho a estar solo, esto es, apartado de observación (lo que podemos llamar seclusión o tranquilidad); como secreto; como un ámbito de no injerencia; como autodeterminación y autonomía; como el derecho a restringir información sobre uno mismo; como territorialidad, lo que comprende seclusión y secreto, y también como un derecho a la imagen. Es evidente que algunas de estas nociones se superponen o implican entre sí.

Tenemos por ejemplo el caso de María Rodríguez, quien en un artículo denominado "Protección de la Vida Privada: Líneas Jurisprudenciales", publicado en la Revista Chilena de Derecho, Vol. 26 N° 3: (pp. 719-744), ordena la jurisprudencia en seis grupos: 1. Información comercial (casos contra Dicom o el Boletín Comercial). 2. Propia imagen, cuerpo y nombre (publicaciones de fotografías en diarios, la rectoscopía

en la Clínica Alemana y reportajes de televisión). 3. Edificaciones en altura. 4. Medidas disciplinarias (entidades que han aplicado sanción a socio o miembro). 5. Inviolabilidad de documentos privados. 6. Vida privada y libertad de expresión (casos contra medios de comunicación o publicaciones)

Por otro lado tenemos la opinión de Pedro Anguita, quien en el documento "Jurisprudencia Constitucional sobre el Derecho a la propia Imagen y la Vida Privada en Chile (1981-2004): un intento de sistematización" presenta una sistematización de la privacidad en 8 grupos: 1. Derecho a la propia imagen, que comprende: a) Derecho a la propia imagen y vida privada (publicaciones no autorizadas de fotos en la prensa). b) Derecho a la Propia Imagen y Falsa Apariencia (publicaciones que distorsionan la imagen de una persona). c) Derecho a la Propia Imagen y Valor Comercial. 2. Vida privada y principio de la autonomía de la persona (casos de colegios que regulan la apariencia personal de los alumnos). 3. Intimidad corporal (rectoscopía de la Clínica Alemana.) 4. La inviolabilidad de toda forma de comunicaciones privadas. 5. Cámaras ocultas y derecho a la vida privada. 6. Derecho a la vida privada vs. libertad de emitir opinión y de informar (casos de libros o reportajes sobre asuntos que los recurrentes consideran parte de su vida privada). 7. Libertad de informar de los medios de comunicación social sobre casos pendientes de resolución en los Tribunales de Justicia (programas de televisión o reportajes sobre sucesos que están sometidos a la jurisdicción). 8. Derecho a la protección de la vida privada y datos personales

Existen también otros autores que realizan otras categorías, pero en todos ellos existe concenso, ratificado por jurisprudencia de tribunales, que la noción de protección a la vida privada y a la honra de su persona y familia es amplia. Por lo mismo trataremos de mencionar en concreto como existe vulneración y amenaza de este derecho y garantía reconocido en la Constitución que afectan tanto los comuneros mapuches como los que actamos personalmente en este recurso.

Es importante recordar que el software “antorcha” se componía de un programa que busca la interceptación de las comunicaciones privadas, a través del envío, mediante la técnica de “phishing”, de un “malware” por medio de un correo electrónico, y una vez que la víctima accedía al contenido del link enviado, se instalaba esta aplicación y se tomaba control del dispositivo móvil. Sin embargo, adicionalmente se utiliza un servidor web que tiene por finalidad recopilar la información contenida en estos equipos celulares, tales como conversaciones de mensajería instantánea, imágenes y documentos privados de la víctima.

Es en este sentido que Alex Smith a través de la aplicación, deliberadamente afecta directamente la privacidad de las personas infectadas con el software “antorcha”, toda vez que sin autorización previa y por medio de engaño, tal como personalmente lo reconoce en entrevistas realizadas a medios de comunicación social, buscaba extraer información privada, confidencial, secreta, clonándola en su servidor web.

La finalidad, por tanto, es de espionaje. Es un software espía que busca, además de interceptar las comunicaciones privadas, tener acceso a información, conversaciones, documentos, imágenes, etc, que son propias de la vida personal de las personas y que no se encuentran disponibles en fuentes públicas, sino específicamente en fuentes privadas.

Específicamente en el caso de los comuneros mapuches a favor del cual se presenta este recurso de protección, con su aplicación, por tanto, se realizaron múltiples acciones que significaron lesiones directa a la privacidad. Asi nos encontramos que existió recopilación de conversaciones privadas, almacenamiento de las mismas y posterior uso y manipulación de la información privada de las víctimas, incluyendo la revelación de información contenida en sus correos y dispositivos móviles sin que existiera ningún fundamento legal ni mucho menos consentimiento que autorizara este hecho y que afecta la honra y dignidad de estas personas.

La vulneración del derecho a la vida privada de los comuneros aún se encuentra lesionada toda vez que aún no pueden acceder a sus equipos móviles que se encuentran infectados por el software "antorcha" y aún mantienen información privada por parte de Alex Smith y de terceras personas, obtenidas con el software "antorcha" que consideramos ilegal.

Respecto a los recurrentes a nombre propio que presentamos este recurso, con la existencia de este software existe una clara amenaza a nuestra privacidad, toda vez que en forma arbitraria e ilegal, sin que exista de por medio autorización previa, y mediante engaño, es posible que Alex Smith utilice su creación intelectual en nuestra contra, en cualquier momento y sin causa legal que la ampare.

En conclusión, existe amenaza tanto en el acceso a información de nuestra vida privada como en la honra de persona y familia, toda vez que producto de la recopilación, almacenamiento y manipulación, podríamos vernos expuestos a que se revelara esta información a terceros, en forma privada o pública sin control y obviamente todo esto sin autorización expresa para ello, existiendo la posibilidad que incluso aprovecharse de esta información y ser utilizada para posterior estafa, engaño, chantaje, afectar honra, etc.

No existe, por tanto, NINGUNA justificación legal o amparada en la ley que faculte a Alex Smith para que utilizando el software "antorcha", siquiera intente acceder sin nuestro consentimiento y voluntad a información que es considerada privada, mucho menos que acceda, almacene, recopile y getione información amparada por el derecho y garantía constitucional de respeto y protección a la vida privada.

POR TANTO,

A SSI. ROGAMOS:

Por una parte acoger a tramitación el presente recurso de protección y ,en definitiva, restablecer el imperio del Derecho amparando a favor de los comuneros mapuches JAIME EDUARDO HUENCHULLÁN CAYUL, ERNESTO LINCOYAM LLAITUL PEZOA, CLAUDIO ANTONIO LEIVA RIVERA, MARTÍN DAMIÁN CURICHE CURIQUEO, FIDEL LAUTARO TRANAMIL NAHUEL, DAVID EDUARDO CID AEDO, HÉCTOR JAVIER LLAITUL, CARRILLANCA, y RODRIGO NAZARIO HUENCHULLÁN CAYUL, porque todos ellos sufrieron y se mantiene la privación y perturbación de sus derechos y garantías constitucionales del artículo 19 N°5, que garantiza la inviolabilidad del hogar y de toda forma de comunicación privada y del artículo 19 N°4, que garantiza el respeto y protección a la vida privada y a la honra de la

persona y su familia; y por otra parte, acoger a tramitación el presente recurso de protección y, en definitiva, restablecer el imperio del Derecho de los recurrentes a nombre propio, esto es PEDRO HUICHALAF ROA, FERMIN LEVIO LLANCAMIL y MAURICIO LLAITUL ACUM, porque con sus actos ilegales y arbitrarios, el recurrido ALEX GUILLERMO SMITH LEAY amenaza nuestros derechos y garantías del artículo 19 N°5, que garantiza la inviolabilidad del hogar y de toda forma de comunicación privada y del artículo 19 N°4, que garantiza el respeto y protección a la vida privada y a la honra de la persona y su familia consagrados en la Constitución, con expresa condenación en costas.

PRIMER OTROSI:

Solicitamos se tomen todas las diligencias y medidas de protección posibles, siendo algunas de ellas:

DECLARAR LA ILEGALIDAD del Software “antorcha”, creación intelectual de Alex Smith Leay y de cualquier otro software o aplicación, independiente de su nombre o fantasía, que haya desarrollado Alex Smith y que tenga por finalidad, características y objetivos intervenir comunicaciones privadas.

ORDENAR a Alex Smith Leay a que cese en la creación, desarrollo o perfeccionamiento del software “antorcha” o cualquier otro software que tenga los mismos objetivos, finalidad, características de intervenir comunicaciones privadas, tanto en el presente como para el futuro.

ORDENAR a Alex Smith Leay la eliminación inmediata de cualquier copia que tuviera en su poder del software “antorcha”, en cualquier etapa de producción y de todo software de similares características en cuanto a funcionamiento, finalidad u objetivos que el programa “antorcha”; se ordene a la eliminación de cualquier tipo de documentación, código fuente e instrucciones que tuviera para la posible creación y desarrollo de software “antorcha” o que cumpla iguales objetivos, funcionalidades y características, no importando su nombre de fantasía; y se ordene la cesación de funcionalidad del servidor web asociado al software “antorcha”.

ORDENAR a Alex Smith Leay a eliminar toda información que haya recopilado , almacenado y/o manipulado y que tenga en su poder tras la utilización del software “antorcha”, incluyendo información de los que hayan otorgado su consentimiento para probar la aplicación.

INSTRUIR a la Dirección de Inteligencia de Carabineros para que cesen de utilizar el software “antorcha” y servidor web asociado, en contra de los comuneros mapuches a favor de los cuales es presentado el recurso y en caso de que no se encuentre alguna instrucción legal para su mantenimiento, eliminar la copia de software que tengan en su poder junto con la cesación del servidor web asociado al software “antorcha” .

INSTRUIR a la Dirección de Inteligencia de Carabineros para que no utilicen de ninguna forma el software “antorcha” o de cualquier otro software o aplicación, independiente de su nombre o fantasía, que haya desarrollado Alex Smith o cualquier

otra persona y que tenga como única finalidad interceptar las comunicaciones privadas sin fundamento legal en ninguna otra investigación, presente o futura que se encuentren desarrollando o en vías de desarrollo frente a terceros, aunque se encuentre autorizadas los procedimientos especiales por algún Ministro de Corte de Apelaciones en conformidad a la ley.

INSTRUIR a la Dirección de Inteligencia de Carabineros la eliminación inmediata de cualquier copia que tuviera en su poder del software "antorcha", en cualquier etapa de producción y de todo software de similares características en cuanto a funcionamiento, finalidad u objetivos que el programa "antorcha" y cesación de funcionalidad del servidor web asociado al software "antorcha".

INSTRUIR a la Dirección de Inteligencia de Carabineros a eliminar toda información que haya recopilado , almacenado y/o manipulado y que tenga en su poder tras la utilización del software "antorcha", incluyendo información de los que hayan otorgado su consentimiento para probar la aplicación.

INSTRUIR al Ministerio Público para que tras concluir cualquier investigación judicial asociada, derivada o basada en la llamada "Operación Huracán", solicite a tribunal competente que elimine completamente el software "antorcha" y ordene la cesación de funcionalidad del servidor web asociado al software.

SEGUNDO OTROSI:

Se acompañan los siguientes documentos:

Copia presentada por Felipe Gonzalez Soto, Fiscal Adjunto de la Fiscalía de Alta Complejidad de La Araucanía, en antecedentes RUC 1710036300-3, RIT 7228-2017 presentado al Juez de Garantía de Temuco en el que se tiene presente el cierre de la investigación, del caso denominado "Operación Huracán".

Copia en su versión digital del reportaje titulado "Antorcha 3.0: La mano del controvertido "hacker" tras la Operación Huracán" de las periodistas Leslie Ayala y María José Ahumada aparecida en el Diario La Tercera del día 03 de febrero de 2018, donde se menciona por primera vez a ALex Smith.

Copia en su versión digital de la nota de prensa titulada "No hubo manipulación por parte de Carabineros, hubo errores de programación y de protocolos de peritajes" en donde aparece entrevista para "El Mercurio" de Alex Smith donde explicó cómo opera su aplicación "Antorcha" y qué resultados se pueden obtener con ella, escrita por las periodistas Cinthya Carvajal y Andrea Chaparro del día 12 de febrero de 2018.

TERCER OTROSI:

Sírvase US. I. oficiar al Carabineros de Chile para que informe respecto a la situación contractual de Alex Smith Leay, acompañe copia de su contrato en caso de que existiera y que informe las características de sus servicios, funciones y obligaciones

en la institución, esto para poder determinar con certeza rol de Smith, condiciones y características en relación al software que solicitamos sea declarado ilegal. En caso que haya cesado su contrato, acompañar los antecedentes y fundamentos de su término de contrato.

Sírvase US. I. oficiar al Carabineros de Chile, específicamente a la Dirección de Inteligencia Policial de Carabineros de Chile para que informe:

- si ha utilizado el software "antorcha" de propiedad de Alex Smith y la fecha desde cuando ha comenzado a utilizarlo.
- en caso afirmativo, la cantidad de personas (en números, sin necesidad de identificarlas) que han sido "blancos" tentativos y fallidos, es decir, que no han logrado "infectar" con el software "antorcha".
- La cantidad de personas (en números, sin necesidad de identificarlas) que han sido o son actualmente "blancos" exitosos en la implantación del software "antorcha".

La pertinencia de este oficio dice relación con información relevante para confirmar los hechos expuestos en el recurso, como también de efectos que se generarán en caso de que se acoga el presente recurso.

CUARTO OTROSI:

Sírvase US. I. tener presente que los recurrentes Fermin Levio Llancamil y Mauricio Llaitul Acum, designan abogado patrocinante y confieren poder con todas y cada una de las facultades de ambos incisos del art. 7° del Código de Procedimiento Civil, en especial las de percibir y transigir, las que por este acto se dan por íntegramente reproducidas a Pedro Huichalaf Roa, rut [redacted], abogado habilitado para el ejercicio profesional, quien es también recurrente del presente recurso, se encuentra debidamente individualizado y quien asume personalmente el patrocinio y poder para actuar por cuenta propia en la tramitación de la acción constitucional que se ha deducido, fijando como domicilio para estos efectos [redacted]