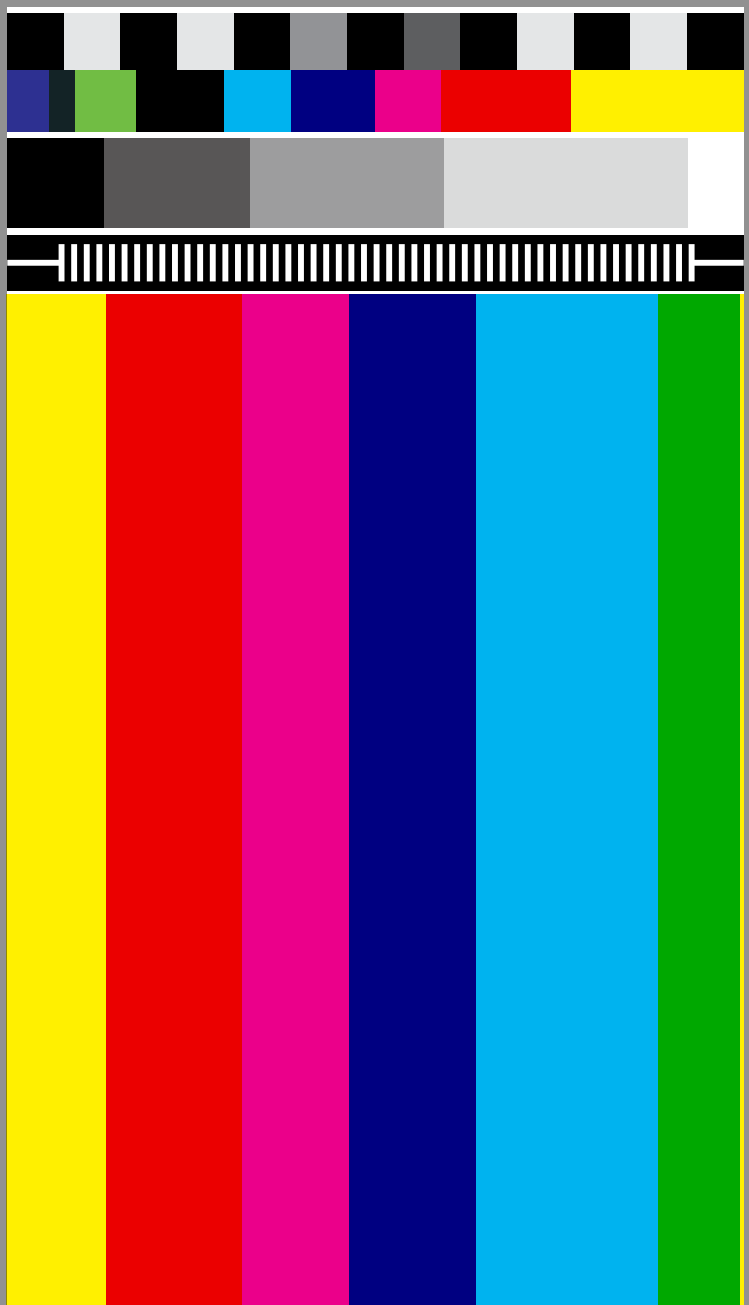
TECNOLOGÍA Y VIGILANCIA EN LA OPERACIÓN HURACÁN: UNA REVISIÓN DEL TRABAJO PERIODÍSTICO REALIZADO EN TORNO AL CASO

VLADIMIR GARAY
ZAK ROGOFF



DERECHOS DIGITALES
América Latina

TECNOLOGÍA Y VIGILANCIA EN LA OPERACIÓN HURACÁN: UNA REVISIÓN DEL TRABAJO PERIODÍSTICO REALIZADO EN TORNO AL CASO

VLADIMIR GARAY
ZAK ROGOFF

DERECHOS DIGITALES
América Latina

Portada y diagramación: Javiera Méndez
Correcciones por María Paz Canales
Septiembre de 2018.

Esta publicación fue posible gracias al apoyo de Privacy International

Derechos Digitales es una organización independiente y sin fines de lucro, fundada en el año 2005 y cuya misión es la defensa, promoción y desarrollo de los derechos fundamentales en el entorno digital, desde el interés público. Entre sus principales ejes de interés está la defensa y promoción de la libertad de expresión, el acceso a la cultura y la privacidad.

Introducción

El 23 de septiembre de 2017, Carabineros de Chile anunció, con gran despliegue mediático, la detención de ocho dirigentes mapuches, acusados como responsables de dos ataques incendiarios contra camiones forestales ocurridos en el mes de agosto. La principal prueba en contra de los dirigentes eran conversaciones realizadas a través de aplicaciones de mensajería, como WhatsApp, interceptadas por la policía. A pesar de que las conversaciones fueron ampliamente difundidas en los medios de comunicación,[1] no se entregaron mayores detalles respecto a las técnicas empleadas para acceder a ellas. El operativo fue bautizado por Carabineros como "Operación Huracán".

Cuatro meses después, el caso daba un vuelco radical. Ante la sospecha de que las pruebas utilizadas para responsabilizar a los dirigentes mapuches habrían sido falsificadas e implantadas, la fiscalía inicio una investigación contra Carabineros por montaje. Hoy, el ex director de inteligencia de Carabineros, General (R) Gonzalo Blu, el Capitán (R) Leonardo Osses, segundo al mando de la Unidad de Inteligencia Operativa Especializada (UIOE) de La Araucanía, y Álex Smith, civil que habría creado las herramientas que supuestamente se habrían utilizado para acceder a las conversaciones –entre otros funcionarios– , se encuentran desvinculados de Carabineros, formalizados criminalmente y con detención preventiva, mientras se investiga el caso.

El interés de los medios de comunicación por Operación Huracán ha tenido como consecuencia abrir una ventana hacia un territorio usualmente opaco, como es la vigilancia estatal en Chile. Poco sabemos respecto al modo en que se desarrolla esta actividad en el país, qué capacidades existen, qué herramientas se utilizan o cómo operan. Si bien estamos lejos de tener una panorámica completa, resulta sumamente interesante el modo en que los distintos trozos –escuetos, parciales, inconexos– adquieren sentido a la luz de la investigación y los estudios ya realizados en la materia.

Si bien puede parecer contradictorio intentar dilucidar certezas a partir de una operación completamente desacreditada como Huracán, lo cierto es que en el trabajo periodístico que se ha realizado sobre ella se asoman atisbos de elementos verosímiles que, al ser reunidos y analizados en conjunto, son coherentes con aprensiones que los expertos han levantado en numerosas oportunidades respecto a la vigilancia en Chile. Se demuestra de esta forma que no se trata de miedos infundados o de situaciones meramente hipotéticas, sino que, ante la falta de claridades legales, contrapesos fuertes y posibilidades de fiscalización, los abusos en el uso de las capacidades de vigilancia ocurrirán.

La información aquí compilada busca ejemplificar tanto prácticas ilegales como aquellas que caen en una problemática área gris conforme a la normativa hoy vigente, con miras a poder

---

1 Ver http://www.t13.cl/videos/nacional/video-detalles-operacion-huracan y http://www.emol.com/noticias/Nacional/2017/09/26/876726/Operacion-Huracan-Guluche-y-viernes-de-fuego-los-conceptos-usados-para-coordinar-ataques-incendiarios.html

diseñar recomendaciones que permitan subsanar estas situaciones en el marco del respeto a los derechos fundamentales.

Junto con ello, permite dar cuenta de una problemática mayor, que es el modo en que ciertos grupos han sido criminalizados, y el poder que tiene el uso de ciertas herramientas tecnológicas por parte de la policía, hoy bajo escaso escrutinio público o de órganos de control. Todo ello conduce a la exacerbación de la mirada vigilante y prejuiciada, pasando por encima del derecho a la igualdad ante la ley, con consecuencias severas para el ejercicio de derechos de los grupos específicos que son foco de tal vigilancia.

Escuchas telefónicas

Uno de los aspectos más relevantes descubiertos en el marco de las investigaciones periodísticas sobre Huracán es una extensa operación de interceptaciones telefónicas a cargo de la Unidad de Inteligencia Operativa Especializada (UIOE) de la Araucanía.

La Constitución Política de la República de Chile establece, en su artículo 19 nº 5, la inviolabilidad de toda comunicación privada, las que solo pueden interceptarse, abrirse o registrarse en los casos y formas determinados por ley. El artículo 222 del Código Procesal Penal detalla las circunstancias y formas en que las comunicaciones telefónicas pueden ser interceptadas. Para ello, deben existir sospechas fundadas de la participación o autoría en un hecho que pudiera merecer la pena de crimen.

Por su parte, el artículo 24 de la ley 19774, sobre el sistema de inteligencia del Estado, considera la interceptación telefónica como uno de los procedimientos especiales de obtención de información de fuentes cerradas, que puede ser invocado cuando determinada información sea estrictamente indispensable para el cumplimiento de los objetivos del sistema y no pueda ser obtenida de fuentes abiertas. Estos procedimientos están limitados exclusivamente a actividades de inteligencia y contrainteligencia relacionadas al terrorismo, el crimen organizado y el narcotráfico. Para proceder, se requiere la firma de un ministro de la Corte de Apelaciones.

Pero como señala a la prensa Rodrigo Román, abogado defensor de algunos de los dirigentes mapuches inculpados en la Operación Huracán, la ley de inteligencia "autoriza intervenciones de manera muy ligera y permite interceptar conversaciones a diestra y siniestra, la ley se interpreta de manera muy laxa".[2]

En el marco de las actividades realizadas por la Unidad de Inteligencia Operativa Especializada (UIOE) de La Araucanía, un reportaje publicado por CIPER señala que entre el año 2016 y el 2018 se intervino un número indeterminado de teléfonos, que se estima se encontraría en algún punto entre los 200 y los 1000.[3]

Los teléfonos son de dirigentes mapuches, pero también de políticos, jueces, fiscales, abogados, actores y periodistas; la mayoría sin relación con la causa mapuche. El reportaje consigna que miembros de Inteligencia reconocieron a CIPER que esas escuchas muchas veces eran ilegales. En aquellos casos donde se ha logrado establecer la existencia de una autorización judicial, habría sido firmada por el ministro de la Corte de Apelaciones de Temuco, Aner Padilla, quien el 9 de agosto de 2017 autorizó a la Dirección Nacional de Inteligencia de Carabineros intervenir 33 celulares. Once de esos teléfonos pertenecían a dirigentes ma-

---

2 http://www.elmostrador.cl/noticias/pais/2018/03/20/el-rol-de-los-magistrados-que-autorizaron-las-intervenciones-telefonicas-de-la-operacion-huracan/

3 https://ciperchile.cl/2018/04/05/operacion-huracan-la-secreta-casa-donde-se-hacian-centenares-de-escuchas-telefonicas-ilegales/

puche investigados en la *"Operación Huracán"*. Se desconoce a quién pertenecían los otros 22. El 7 de septiembre, el ministro Padilla renovó ese permiso, ahora para 23 teléfonos.[4]

Hoy, parece ser que los servidores donde se almacenaba la información obtenida de los teléfonos interceptados, incluidos aquellos autorizados por Padilla, habrían desaparecido. Se desconoce su paradero y específicamente qué información que contenían.[5]

Sin embargo, parte de la información recabada se filtró a la prensa; o, como bien precisa CIPER, "la entregaron quienes tenían acceso a esos audios: los funcionarios que estaban a cargo en la UIOE de las escuchas telefónicas".[6] Se trata particularmente de una conversación telefónica entre el actor Daniel Alcaíno y su pareja, sobre un tópico no relacionado a la causa investigada, ni a la lucha reivindicatoria mapuche. La interceptación se habría justificado por un supuesto financiamiento del actor a los atentados, desestimado por la justicia.[7] Cabe recalcar que la información publicada tiene carácter sensible y carece de relevancia pública. Cabe preguntarse respecto al modo en que el Ministro Padilla sopesó la petición de intercepción a Alcaíno y por qué decidió autorizarla.

Acceso a metadatos telefónicos

El artículo 222 del código procesal penal obliga a las empresas telefónicas y de comunicaciones a mantener a disposición del Ministerio Público un listado actualizado de sus rangos autorizados de direcciones IP y un registro, no inferior a un año, de los números IP de las conexiones que realicen sus abonados.

Diversas instituciones en materia de derechos humanos han declarado que la interceptación, recolección y uso de metadatos interfiere con el derecho a la privacidad, incluyendo al Relator Especial de la ONU sobre libertad de expresión, el Relator Especial de la ONU sobre la lucha sobre la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo y el Alto Comisionado para los Derechos Humanos.[8] El Comité de Derechos Humanos de la ONU ha confirmado que las políticas de retención de datos constituyen una interferencia con el derecho a la privacidad y que, como regla general, los estados deben "abstenerse de imponer la retención obligatoria de datos por parte de terceros".[9]

---

4 https://ciperchile.cl/2018/04/05/operacion-huracan-la-secreta-casa-donde-se-hacian-centenares-de-escuchas-telefonicas-ilegales/

5 https://ciperchile.cl/2018/04/05/operacion-huracan-la-secreta-casa-donde-se-hacian-centenares-de-escuchas-telefonicas-ilegales/#h2_1

6 https://ciperchile.cl/2018/04/05/operacion-huracan-la-secreta-casa-donde-se-hacian-centenares-de-escuchas-telefonicas-ilegales/

7 http://www.24horas.cl/nacional/daniel-alcaino-por-operacion-huracan-si-me-nombran-yo-me-querello-2645195

8 "El Derecho a la privacidad" Comunicación conjunta de Derechos Digitales, Ciudadano Inteligente, Fundación Pro Acceso, y Privacy international al Examen Periódico Universal 32o período de sesiones – Chile. P. 6

9 UN Human Rights Committee, Concluding Observations of the Fourth Periodic Report of the United States of America, UN Doc. CCPR/C/USA/CO/4, 23 April 2014, para. 22.

La investigación periodística de Nicolás Sepúlveda establece que la UIOE tenía acceso a Vigía, el software utilizado por todas las compañías de telecomunicaciones en Chile para administrar el registro de los metadatos de las comunicaciones, incluyendo los datos de llamadas recibidas, realizadas, la duración de estas y la antena que se utilizó para concretarlas. Pero no solo eso, sino que además el software conservaría también los mensajes de texto de un número telefónico. [10]

Llama poderosamente la atención el modo en que los miembros de la Unidad tendrían acceso a los metadatos:

> Si el sistema se ocupa legalmente, un juez debe autorizar el acceso a esta información. Pero distintas personas que han integrado o integran equipos de inteligencia relataron a CIPER la existencia de una vía paralela. Como en casi todas las compañías telefónicas los encargados de la seguridad y de dar acceso a las interceptaciones son oficiales de Carabineros en retiro, se posibilitan los tratos privados entre efectivos de inteligencia y ejecutivos de las compañías telefónicas para acceder a información absolutamente privada de ciudadanos sin autorización.[11]

Poco se sabe respecto al modo en que funciona la plataforma que recopila los metadatos comunicacionales, por lo que es difícil tener una idea clara respecto a la factibilidad de la información presentada por CIPER. A pesar de ello cabe la pregunta respecto a los modos en que las policías, el Ministerio Público y las propias compañías de telecomunicaciones pueden controlar y registrar los accesos al sistema y alertar frente a usos indebidos, abusivos e ilegales a la información.

Uso de spyware y phishing

Uno de los aspectos más bullados sobre la Operación Huracán dice relación con el uso de spyware. Particularmente porque existe una duda razonable de que Antorcha, el software supuestamente creado por Álex Smith y usado por la UIOE, realmente existe, lo que sustenta la tesis de la fabricación de pruebas y el montaje.

Pero para efectos de este análisis, la existencia (o no) de Antorcha es menos relevante que la intención de utilizar este tipo de herramientas: si carabineros hubiese podido acceder a un software más sofisticado, lo habría hecho, y la discusión respecto a la validez del uso de este tipo de herramientas sería la misma.

Según detalla el capitán (R) Leonardo Osses, las incursiones de Carabineros en el uso de Spyware está relacionada a la necesidad de acceder a "información a la que no podemos te-

---

10 https://ciperchile.cl/2018/04/05/operacion-huracan-la-secreta-casa-donde-se-hacian-centenares-de-escuchas-telefonicas-ilegales/

11 https://ciperchile.cl/2018/04/05/operacion-huracan-la-secreta-casa-donde-se-hacian-centenares-de-escuchas-telefonicas-ilegales/

ner acceso con los métodos comunes".[12] En su relato, Osses explica que estarían tras la pista de individuos que se adjudicaban ataques incendiarios. Se desprende de su narración de que estas personas habrían estado intervenidas telefónicamente:

> Pero en muchas escuchas ellos señalaban que "no hablemos por teléfono, porque estamos intervenidos. Así que hablemos por WhatsApp o hablemos por Telegram", y esa era nuestra limitante, porque nosotros sabíamos que ellos se comunicaban por ese tipo de mensajería y lo complicado es que no sabíamos cómo llegar a esa información.[13]

En otra entrevista, Álex Smith agrega:

> Nació la necesidad de intervenir redes sociales. Lo más fácil para mí era el pishing. Comenté que se podía hacer y pregunté si era legal, me dijeron que por una ley, la de inteligencia, sí. Como era legal, empezamos a enviar pishing a distintos blancos.

A pesar de lo señalado por Smith, la legalidad de la medida es dudosa. Por una parte, la ley 19774 establece la posibilidad de interceptar comunicaciones, sistemas y redes informáticas, limitados exclusivamente a actividades de inteligencia y contrainteligencia relacionadas al terrorismo, el crimen organizado y el narcotráfico, con autorización de un ministro de la Corte de Apelaciones.

En efecto, el ministro de la Corte de Apelaciones de Temuco, Aner Padilla, firmó una autorización para la interceptación de los mensajes de nueve teléfonos móviles, a petición de Gonzalo Blu, según consigna una nota publicada en El Mostrador.[14] Un elemento importante es que la autorización fue firmada con fecha 7 de septiembre, mientras que la última comunicación interceptada se realizó el 29 de agosto. Es decir, la interceptación se habría realizado sin autorización legal, la que se habría conseguido a *posteriori*.

Otra cuestión que es importante recalcar es que las facultades otorgadas por la ley 19774 para la interceptación de comunicaciones electrónicas se limita a actividades de inteligencia y la información recabada no puede utilizarse en un proceso penal.

El informe emitido por la Policía de Investigaciones en el marco del proceso para esclarecer la acusación de montaje contra los funcionarios de la UIOE, junto con señalar de forma categórica que Antorcha nunca existió, establece que el uso de phishing constituye un delito

---

12 https://www.latercera.com/reportajes/noticia/capitan-r-leonardo-osses-la-fiscalia-siempre-estuvo-al-tanto-lo-haciamos-antorcha/78391/

13 https://www.latercera.com/reportajes/noticia/capitan-r-leonardo-osses-la-fiscalia-siempre-estuvo-al-tanto-lo-haciamos-antorcha/78391/

14 http://www.elmostrador.cl/noticias/pais/2018/03/20/el-rol-de-los-magistrados-que-autorizaron-las-intervenciones-telefonicas-de-la-operacion-huracan/

informático,[15] tipificado en por la Ley 19.223, ya que la víctima habría sido objeto de un ataque informático para obtener credenciales personales.
Cabe mencionar acá que una de las técnicas utilizadas para la diseminación de software malicioso era la creación de falsos perfiles en redes sociales, particularmente Facebook, con el fin de engañar a los blancos y enviar un keylogger para obtener sus credenciales de acceso a distintas plataformas. No está claro el éxito de la medida.[16]

Otra de las técnicas de phishing utilizadas era la preparación de correos electrónicos con programas maliciosos disfrazados como software inofensivo. Un aspecto interesante respecto a esta técnica lo señala Álex Smith en una entrevista concedida a La Tercera: "a veces no teníamos correo y se conseguían ellos los datos de los blancos con Banco Estado".[17] No queda claro en la nota bajo qué figura Banco Estado entregaría esta información, si se trata de una política institucional o –al igual que con el acceso a la base de metadatos administrada por las empresas de telecomunicaciones– se hace de forma informal, aprovechando los contactos dentro del banco para acceder a información personal de los clientes.

Adquisición secreta de herramientas tecnológicas

Otro de los aspectos interesantes revelados en el marco de las investigaciones periodísticas sobre Huracán dice relación con la adquisición de software especializado, particularmente Oxygen Forensic Rugged Kit. Se trata de un programa utilizado para hacer peritaje forense de equipos móviles y habría sido utilizado para analizar los equipos de los dirigentes mapuches detenidos en el marco de la Operación Huracán.

Si bien puede que la herramienta no sea en si misma controversial, lo que si llama la atención es el relato del modo en que fue adquirida. Gonzalo Iván Paredes Quezada, propietario de la empresa Xmartlab declara a La Tercera:

> El 1 de septiembre, el mayor Marín llegó "con el dinero en efectivo equivalente al monto cotizado, con el objeto de adquirir el producto seleccionado. Recuerdo que al momento de pagar el producto el mayor Marín extrajo desde una maleta un sobre plástico sellado con el nombre del 'Banco Central', que contenía billetes con una nominación de $20.000. Al abrirlo se contabilizó la suma de $20.000.000. Luego extrajo distintos un fardo de billetes de $10.000 (diez mil pesos) y pagó la diferencia".[18]

La adquisición de una herramienta por 21 millones de pesos pagados en efectivo solo puede tener como finalidad evitar dejar rastros sobre la transacción. Puesto que no existe nin-

---

15 https://www.latercera.com/reportajes/noticia/antorcha-nunca-existio-las-claves-del-ultimo-informe-la-operacion-huracan/154002/

16 https://ciperchile.cl/2018/04/05/operacion-huracan-la-secreta-casa-donde-se-hacian-centenares-de-escuchas-telefonicas-ilegales/

17 https://www.latercera.com/la-tercera-pm/noticia/extasis-derrota-del-super-agente-smith-no-mala-persona-cai-huevon/207299/

18 https://www.latercera.com/la-tercera-pm/noticia/software-espia-carabineros-compro-efectivo-usado-profesor-smith-21-millones-billetes/196428/

guna obligación para que las instituciones legalmente habilitadas a realizar actividades de inteligencia declaren públicamente la compra de sus herramientas, no hay modo de saber a ciencia cierta con qué capacidades cuentan ni cómo las utilizan.

Esto es relevante, puesto que muchas de las herramientas hoy disponibles en el mercado presentan capacidades que infringen o podrían infringir las limitaciones legales a sus usos. Como tampoco existe una obligación de entregar detalles respecto al modo en que las actividades de inteligencia se realizan, en la práctica no es posible efectuar ningún tipo de control sobre la legalidad de las actividades de vigilancia estatal que se realizan en Chile.

Esta situación ya se había hecho manifiesta hace un par de años atrás, cuando la filtración de información confidencial de la empresa italiana Hacking Team entregó detalles sobre la adquisición que la Policía de Investigaciones había hecho del software Galileo, por un monto superior a los dos millones de euros. Aunque primero la transacción fue negada, ante la evidencia la PDI se vio obligada a reconocerla. No es mucho más lo que se sabe respecto al uso específico que la policía habría dado a esta herramienta, altamente intrusiva y legalmente cuestionable.

En el marco de la investigación periodística se pudieron conocer algunas de las herramientas con las que cuenta Carabineros: EGO, para interceptación telefónica ("y que tendría capacidad de interceptar comunicaciones vía internet. Esta función, en términos formales, no habría sido usada porque es ilegal"); y UFED, "un programa fabricado por Cellebreti. Según su promoción, permite extraer de cualquier teléfono registros de llamadas, incluso los borrados de la tarjeta SIM, contactos, fotografías, vídeos, archivos de sonido, información de localización de la SIM, geoetiquetas gráficas en Google Maps.[19]

Vigilancia en redes sociales

Otro de los aspectos que más ha llamado la atención dentro de las investigaciones realizadas en torno a la polémica Operación Huracán dice relación con el monitoreo y vigilancia en redes sociales.

En un reportaje titulado "Los periodistas que fueron objeto de espionaje electrónico de Carabineros"[20] y publicado en CIPER, el periodista Nicolás Valenzuela señala que "en la unidad de Inteligencia de La Araucanía (UIOE) los carabineros estaban obsesionados por saber quiénes eran los periodistas que publicaban noticias sobre ellos, y la identidad de las fuentes que les entregaban los antecedentes". El encargado de recabar la información era Álex Smith.

En términos generales, el reportaje narra dos tipos de situaciones distintas, pero entrelazadas; y, como siempre es el caso con las acciones de Smith, el límite entre lo que es plausible y lo que no se vuelve difuso y confunde. Por un lado, se describen distintos casos en los cuales

19 https://www.latercera.com/la-tercera-pm/noticia/huracan-las-declaraciones-claves-descifran-quienes-espiaba-carabineros/124587/

20 https://ciperchile.cl/2018/03/07/los-periodistas-que-fueron-objeto-de-espionaje-electronico-de-carabineros/

funcionarios de Carabineros solicitaron a Smith recabar información respecto a los autores de información incómoda para la institución o el Gobierno, publicada en medios de comunicación. Se trata de información pública, como direcciones URL y cuentas de redes sociales utilizadas por los medios, así como los nombres de los periodistas que firman la nota o de quienes la publican.

Junto con ello, Álex Smith también proveía información supuestamente interceptada por su software, que incluía conversaciones vía chat entre periodistas y fuentes anónimas, geolocalización de los lugares desde los cuáles se realizaron publicaciones y desanonimización de autores. Consultados, los periodistas aludidos desmienten tajantemente esta parte de las investigaciones de Smith, del mismo modo en que el resto de la información compilada gracias a su software (de existencia dudosa) ha sido descartado.

Respecto al monitoreo y compilación de información abierta publicada en internet, si bien los reportajes en torno a Huracán no indagan mayormente en este último punto, más allá de explicar el trabajo de Álex Smith, otro incidente no relacionado a la causa, ocurrido a fines de agosto podría aportar más pistas al respecto:

En el marco de una investigación policial por una presunta amenaza denunciada por la ministra secretaria general de Gobierno, Cecilia Pérez, Carabineros confirmó la existencia en el OS-9 de un equipo especializado para detectar amenazas en las redes sociales.

Según consigna La Tercera: [21]

> El equipo está conformado esencialmente por cuatro ingenieros, quienes realizan "ciberpatrullajes" en las diferentes redes sociales, para encontrar conductas delictuales en internet (...) La vocera del OS-9, teniente Javiera García, explicó que este equipo "constantemente mantiene monitoreos o patrullajes virtuales revisando muchas redes sociales. Cuando hay algún comentario que indica directamente la intención de agredir gravemente a una persona, como, por ejemplo, un te voy a matar, se enciende la alerta que la configura como una amenaza a considerar y a investigar junto al Ministerio Público".
>
> Posteriormente, explicó, se contacta a la víctima de las amenazas y "se lleva a cabo el rastreo, aunque es mucho más fácil y más rápido cuando existe la denuncia, porque ahí se entregan antecedentes por mensajería interna u otros de contenido más explícito".

Consultada para esta investigación, la vocera del OS-9 explicó que, en el marco de investigaciones en curso, el OS-9 realiza búsquedas de información relevante desde fuentes abiertas en internet, como pueden ser perfiles, páginas y grupos en redes sociales, como Facebook, o sitios web dedicados a la compra-venta, por ejemplo, en el caso del trabajo realizado por el grupo encargado de investigar causas relacionadas con el robo de camiones.

---

21 https://www.latercera.com/nacional/noticia/desconocido-ciberpatrullaje-carabineros-las-redes-sociales/299027/

Parte importante del trabajo se centra en establecer lo que el OS-9 denomina "redes de apoyo" y "redes familiares": a través de las interacciones en redes sociales, Carabineros determina con quiénes se comunica y se relaciona la persona que está siendo investigada. Está información es analizada a la luz de otros datos, como los antecedentes penales de las personas que se comunican con el la persona que está siendo monitoreada, y en base a eso se decide (o no) incluirles en la investigación. Esta información está siendo compilada en una base de datos, cuyo desarrollo técnico se encuentra todavía en construcción, al igual que los protocolos que rigen los "ciberpatrullajes".

Además de perfiles personales, desde el OS-9 explican que también monitorean frecuentemente algunas agrupaciones o colectivos que están investigando, como es el caso de barras de fútbol, colectivos "anarquistas" o agrupaciones feministas (este último, rastreando muestras de violencia en línea que puedan dar pistas respecto a los responsables de un ataque a tres mujeres ocurrido en el marco de una manifestación a favor del aborto, a fines de julio).

Las actividades de ciberpatrullaje están apoyadas por un equipo de cuatro ingenieros, dedicados a hacer peritajes, como determinar una dirección IP o geolocalizar una fotografía.

En base a los antecedentes recabados, Carabineros puede pedir autorización para escalar las medidas de vigilancia (seguimientos, interceptación de comunicaciones, etc.); de igual forma en caso de que la configuración de privacidad de la fuente de la información cambie y no sea posible seguir accediendo.

Una reflexión final

Como señalábamos al comienzo, la idea de este pequeño ejercicio consistía en poder analizar la información producida en torno a la Operación Huracán, a la luz del análisis sobre las deficiencias en el sistema legal chileno en relación a las prácticas de vigilancia estatal. La idea era poder ir más allá de lo anecdótico y plantear la pregunta respecto a cómo fue posible que esto hubiese ocurrido en primer lugar; a la luz del trabajo y la reflexión previa en torno a la vigilancia estatal, queríamos ver de qué manera encaja un caso como Huracán.

Lo más interesante de este análisis es, precisamente, el modo en que las aprensiones previamente levantados en torno a distintas falencias de la regulación sobre vigilancia estatal en Chile se ven confirmados a partir del reporteo realizado en torno a Operación Huracán.

Así mismo, llama la atención el amplio espectro de situaciones de naturaleza distinta que es posible identificar en el análisis sobre Operación Huracán, desde el almacenamiento masivo de metadatos comunicacionales hasta la falta de transparencia en torno a la adquisición de tecnología de vigilancia y análisis.

En ese sentido, una de las cuestiones que parece relevante mencionar es que Operación Huracán no es simplemente el resultado de funcionarios policiales empeñados en falsificar pruebas. El hecho de que se haya elegido falsificar pruebas supuestamente obtenidas en el marco de la interceptación de comunicaciones en internet pone de manifiesto que la falta de claridades legales, contrapesos fuertes y la posibilidad de fiscalizar, fue una de las razones que permitió el abuso en primer lugar. Es posible considerar de que si existiesen mayores controles sobre las actividades de vigilancia por medios electrónicos, los ocho dirigentes mapuches nunca habrían sido detenidos.

De esta manera, podríamos concluir que la creación de un marco regulador fuerte en torno a una actividad tan delicada y potencialmente lesiva de derechos fundamentales como es la vigilancia a través de las nuevas tecnologías, vuelve más seguro al sistema completo, asegurando que las actividades de vigilancia sean proporcionales, evitando que personas inocentes vean su derecho a la privacidad arbitrariamente diezmado y evitando que las instituciones encargadas de ejecutar la vigilancia en forma legal y excepcional, se vean expuestas por la acción de funcionarios inescrupulosos.

De esta manera, se vuelve prioritario mejorar la legislación, generando mayor transparencia en torno a las operaciones y técnicas de investigación, creando instancias de fiscalización independientes respecto al modo en que la vigilancia es ejecutada y contrapesos fuertes que permitan que los derechos de las personas sean respetados a cabalidad. De esta manera es posible asegurar una convivencia más justa y democrática.


DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina