LAS REVELACIONES DE HACKING TEAM
¿Qué consecuencias tienen para Chile?

Gisela Pérez de Acha - Derechos Digitales

Borrador

A. INTRODUCCIÓN

Perseguir delitos, cometiendo delitos. Salvaguardar la democracia, con secretismo y opacidad. Hacer cumplir la ley, aprovechando los vacíos regulatorios de la misma. Esa es la lógica de Hacking Team: la empresa italiana encargada de vender y comercializar uno de los *softwares* de vigilancia más invasivos que se conocen a nivel masivo. Lo vende únicamente a los gobiernos del mundo, y su mensaje de propaganda es bastante claro:

> *"El ciberespacio no tiene fronteras. Su sospechoso puede estar en cualquier lugar hoy, pero sus manos están atadas en cuanto sale del país. No podemos evitar que se muevan, pero ¿cómo puede continuar persiguiéndolos? Necesita un sistema que rodee las comunicaciones cifradas, que pueda recoger información relevante de cualquier dispositivo, y que continúe monitoreando a las personas de su elección donde quiera que estén. Remote Control System hace precisamente eso."*[1]

Galileo y DaVinci, los nombres comerciales de este programa de monitoreo específico, *Remote Control System* [RCS] se esconden detrás de la ilusión de un objetivo legítimo: combatir la delincuencia. Sin embargo, por la misma naturaleza secreta de las actividades de espionaje, poco sabíamos de qué trataba este *software,* cuáles eran sus alcances y posibles daños.

Así era hasta que el domingo 5 de julio de 2015, se expusieron públicamente 400 GB de información de Hacking Team. Los documentos incluyen facturas, correos electrónicos, datos fiscales y código fuente, entre otros archivos.

La traducción literal de RCS es "Sistema de Control Remoto", y se llama así porque actúa a manera de virus, y una vez que los dispositivos son infectados, pueden controlarse de manera remota, es decir, a distancia. Lo que distingue a RCS con el

[1] Traducción libre de Remote Control System. Galileo Overview. Hacking Team. http://www.scribd.com/doc/286613275/Hacking-Team-Brochure-for-RCS-Galileo

resto de formas de vigilancia tradicionales –como las escuchas telefónicas– es que no solo tiene acceso a conversaciones y comunicaciones, sino que además puede capturar todo tipo de información, imágenes y datos que se encuentren en la computadora de las personas infectadas, sin que sea necesario que los mismos viajen por internet.[2] Es el equivalente a tener un funcionario de gobierno mirando por encima de nuestros hombros, y registrando toda nuestra actividad en computadoras o teléfonos celulares. Inclusive, RCS permite tener acceso a correos y comunicaciones cifradas, además de poder copiar información del disco duro de un dispositivo, grabar llamadas de Skype, mensajes instantáneos y saber qué contraseñas se escriben en cada sitio y en cada momento. Por si fuera poco, tiene acceso y puede activar cámaras y micrófonos.

Con la filtración supimos que seis países de América Latina son clientes de Hacking Team: Brasil, Chile, Colombia, Ecuador, Honduras, México, Panamá y Venezuela. Adicionalmente, Argentina, Guatemala, Paraguay y Uruguay negociaron con la empresa, aunque nunca concretaron la compra.

Hacking Team basa la venta de sus productos en la legalidad de los mismos. Inclusive en sus términos y condiciones, la empresa se jacta de no vender su producto a países que "facilitan graves violaciones a derechos humanos", sin embargo, las propias filtraciones dieron cuenta de que su tecnología se estaba vendiendo a países con reconocidas violaciones sistemáticas de derechos humanos como Egipto, Sudán o Azerbaiyán.[3]

Al hacer un análisis legal de todos los países implicados encontramos que no existen regulaciones específicas para Galileo o DaVinci, o bien las reglas existentes no son plenamente aplicables. Pero su existencia, adquisición y uso exigen una discusión abierta respecto a qué estándares legales deben regir este tipo de tecnología.

Dado el historial de autoritarismos y violaciones a derechos humanos en la región, surgen las siguientes preguntas: ¿Qué implica esta compra para las democracias de estos países? ¿Cómo se utiliza este tipo de software? ¿Cuáles son sus alcances y posibles riesgos? ¿Es legal este tipo de espionaje? ¿Hay sanciones en caso de que no lo sea?

---

[2] Informe de Citizen Lab. Mapping Hacking Team's Untracable Spyware.
https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/#2

[3] Electronic Frontier Foundation. Hacking Team Leaks Reveal Spyware Industry's Growth, Negligence of Human Rights
https://www.eff.org/deeplinks/2015/07/hacking-team-leaks-reveal-spyware-industrys-growth

A continuación, estudiaremos los componentes técnicos del *software* de Hacking Team para saber cómo se infecta, con qué criterios, a quiénes y qué implicaciones o peligros se presentan. Posteriormente, compilamos todos los hechos relativos a Hacking Team en Chile para hacer un análisis legal en cuanto a facultades y debido proceso en este país.

Entre sus clientes están varios países que atraviesan una grave crisis de derechos humanos, y que no tienen controles democráticos suficientes al interior de sus instituciones. A pesar de la filtración y la publicación de los contratos entre Hacking Team y distintos organismos gubernamentales, en ningún país en América Latina (salvo Panamá) se han abierto investigaciones al respecto.

Nuestra conclusión es que al no estar expresamente regulado, y por ser altamente intrusivo, el *software* de espionaje que vende la empresa es contrario a derechos humanos en todos los países, y por lo tanto ilegal. En otras palabras, su uso va más allá de la ley, pues aprovecha el vacío que se produce entre la regulación de las interceptaciones pasivas de comunicaciones, y las pesquisas o búsquedas físicas.

Operar en la ilegalidad y bajo esquemas que violan derechos humanos, amerita una sanción penal en cada uno de los países que estudiamos.

B. TECNOLOGÍA

Antes de continuar con el análisis legal de las implicaciones del *Remote Control System* de Hacking Team, procuraremos exponer de manera simple cómo funciona su tecnología y qué implicaciones tiene la misma.

Una buena explicación proviene de los propios manuales de uso de la empresa, publicados por el diario *The Intercept* en octubre de 2014.[4] En ellos, Hacking Team detalla instrucciones minuciosas para los técnicos, administradores y analistas sobre cómo infectar un dispositivo y echar a andar los mecanismos de espionaje. La siguiente explicación toma estos manuales como base.

1. ¿Cómo se infecta?

El *software* puede instalarse de varias formas, y cada uno es efectivo contra ciertos dispositivos y sistemas operativos, dependiendo del contexto y las características de los mismos. Sin embargo, algo tienen en común: que todos requieren un acto de

[4] The Intercept, Secret Manuals Show the Spyware Sold to Despots and Cops Worldwide. https://theintercept.com/2014/10/30/hacking-team/

“engaño” a la persona infectada. Es decir, no puede instalarse de otra manera. Distintas vías pueden utilizarse para ese resultado.[5]

La primera forma en que puede realizarse la infección es de manera física a través de una unidad USB, si las autoridades tienen acceso físico directo a la computadora. Por ejemplo, en un retén policial, al visitar o allanar un lugar, o realizando un cateo en aeropuertos.

La segunda forma es sin acceso directo al equipo, pero en su entorno, mediante inyecciones que emulan una red de wi-fi, cuando un agente espera en el vestíbulo de un hotel o un café para ganar acceso a la computadora mediante un falso y “gratuito” punto de conexión a internet. Es decir, ofreciéndose como red abierta para quien quiere conectarse a la red.

En tercer lugar, se puede infectar utilizando vías remotas. El tipo más común de infección aquí, es el que contiene el *malware* en un correo tramposo con una falsa invitación, como en el caso del correo con una falsa invitación adjunta para poder infectar un equipo. A los periodistas, les envían correos con adjuntos que sean de una falsa promesa de información en el que al abrir el archivo adjunto, se instala la infección de *malware*.[6]

Otro tipo de vía remota es el *software* que se esconde en descargas legítimas de aplicaciones en celulares, a través del uso de “*exploits*”: códigos que se aprovechan de los errores (*bugs)* en programas comerciales, por ejemplo en el caso de Android. [7] En esta categoría, Hacking Team ofrece la posibilidad de usar un tipo de *exploit* bastante controvertida: los códigos maliciosos secretos (*zero-day*) que explotan fallos de software no conocidos públicamente y que por ende no han sido arreglados, por lo que los afectados no tienen tiempo para reaccionar. De ahí que se les llame *“zero-day”*, en función de este tiempo de reacción, que es prácticamente cero.[8]

---

[5] The Intercept, “Secret Manuals Show the Spyware Sold to Despots and Cops Worldwide”. https://theintercept.com/2014/10/30/hacking-team/

[6] Así ocurrió, por ejemplo, en México, en relación con contiendas políticas intrapartidarias. Animal Político, “El gobierno de Puebla usó el software de Hacking Team para espionaje político”. http://www.animalpolitico.com/2015/07/el-gobierno-de-puebla-uso-el-software-de-hacking-team-para-espionaje-politico/

[7] Morgan Marquis-Boire et. al, “Police Story: Hacking Team’s Government Surveillance Malware”. https://citizenlab.org/2014/06/backdoor-hacking-teams-tradecraft-android-implant/

[8] “Hacking Team, Chile y Ecuador”. https://people.torproject.org/~ilv/ht_chile_ecuador.html

En cuarto lugar, se puede esconder en cualquier tipo de tráfico no cifrado en internet, como por ejemplo, en enlaces a videos de Youtube o Microsoft Live que al momento de ser vistos, infectan el dispositivo.[9]

Por último, puede ser a través de la creación de vínculos de internet y URL maliciosos. Una vez que un funcionario de gobierno sabe qué dispositivo desea infectar, llena un formulario en el sistema de soporte en línea de Hacking Team especificando el tipo de software espía que quiere instalar y de qué manera. Un ingeniero de la empresa se encarga entonces de vincular el software espía a dicho método y le entrega el enlace al funcionario gubernamental, quien deberá engañar a su víctima para que abra el mismo y que se instale el *software* espía en el dispositivo. Generalmente, el enlace provisto por Hacking Team es de ejecución única, es decir, una vez utilizado no volverá a funcionar otra vez.[10]

2. ¿Quién lo opera?

Los operadores –o agentes, como los llama Hacking Team— son siempre funcionarios de organismos gubernamentales que han comprado el *software*. Después de una capacitación por parte de la empresa, son estos quienes operan el espionaje personalizado en cualquiera de los casos.

3. ¿En qué dispositivos funciona?

A través de uno de los métodos señalados con anterioridad, el *software* de espionaje puede implementarse en cualquier computadora con OS X (Apple), o Windows (Microsoft). Y además en cualquier teléfono celular con sistema Android, BlackBerry, iOS (iPhone), Symbian o Windows Mobile.[11]

4. ¿Qué puede verse?

El “analista” —o funcionario de gobierno que tiene acceso y está capacitado para usar el programa— puede acceder y copiar cualquier tipo de información contenida en la computadora o teléfono celular de la víctima. Entre ellas, el manual lista las siguientes: contactos, aplicaciones utilizadas, calendario, llamadas y audios de teléfono, Skype o MSN, cámara y webcam, chat, todo lo copiado al portapapeles, archivos abiertos por la víctima, disco duro, teclas apretadas, mensajes y correos

[9] Después de que The Intercept reveló esta falla en los sistemas de YouTube y Microsoft Live, ambas compañías tomaron medidas para disminuirlo. https://theintercept.com/2014/08/15/cat-video-hack/
[10] “Hacking Team, Chile y Ecuador”. https://people.torproject.org/~ilv/ht_chile_ecuador.html
[11] The Intercept, “Secret Manuals Show the Spyware Sold to Despots and Cops Worldwide”. https://theintercept.com/2014/10/30/hacking-team/

electrónicos, micrófono y audio, clicks del *mouse,* contraseñas, posición geográfica en tiempo real, impresiones, capturas de pantalla y sitios de internet visitados.[12] Además *software* de RCS puede tener acceso a los archivos locales de redes sociales y aplicaciones para *chat* incluyendo Facebook, Viber, WhatsApp, LINE y QQ. En otras palabras: prácticamente todo.

Una vez que se tiene acceso a esto, el programa rastrea los vínculos, lugares y personas que tienen relación con de la víctima infectada, en función de la constancia de contacto que tengan con la misma.

5. ¿Cuál es su funcionamiento técnico?

En el funcionamiento técnico de la red que *Remote Control System* implica, se pueden apreciar tres partes fundamentales[13]:

> 1) Red interna de RCS. Manejada por los organismos gubernamentales (y agentes de los mismos) que compraron el *software* de espionaje. Posee un único punto de acceso público (es decir, que se puede acceder desde internet) llamado Collector.
>
> 2) Collector. Puerto que se encarga de recolectar toda la información recibida desde Internet y enviarla al resto de la red interna de RCS para ser procesada y almacenada. Esto permite un umbral de seguridad adicional pues se instala un "firewall" entre la red interna de RCS y toda la información recibida por los agente
>
> 3) Softwares espía. Se dicen en plural porque para cada "dispositivo", teléfono celular o computadora de la persona infectada, se debe instalar uno distinto. Se distribuyen a través de la red de RCS y su función es recopilar y enviar la información de cada dispositivo a la cadena de Anonymizers.
>
> 4) Anonymizers. Servidores distribuidos geográficamente alrededor del globo (en este caso, A, B y C) cuya función es mantener la comunicación entre los software espía instalados en cada dispositivo y la red interna de RCS de manera anónima. Es decir, entre lo externo e interno de RCS. Para esto, se

[12] Hacking Team, Chile y Ecuador https://people.torproject.org/~ilv/ht_chile_ecuador.html
[13] Manual Hacking Team. RCS 9.6; The hacking suite for governmental interception. System administrator manual https://s3.amazonaws.com/s3.documentcloud.org/documents/1348003/rcs-9-admin-final.pdf

crea una cadena de servidores que transportan la información recolectada desde las víctimas hasta el Collector secuencialmente.

6. ¿Por qué es indetectable?

En el manual, Hacking Team se jacta de que RCS "…crea, configura e instala agentes de software de forma anónima que recopilan datos e información y envían los resultados a la base de datos central para decodificarlos y guardarlos."[14]

Esto funciona de dos formas. Primero, porque los manuales de Hacking Team recomiendan a sus clientes que compren un certificado de Verisign (ahora Symantec), Thawte o GoDaddy, pues estas compañías proveen certificados digitales de seguridad que permiten que el software sea más difícil de ser detectado. [15]

Segundo, porque el mecanismo a través del cual se recolecta la información de la persona espiada, evita el vínculo directo entre el dispositivo infectado y el agente u organismo de gobierno. Por lo mismo, es casi imposible de vincular, y muy difícil de denunciar. Según *The Intercept,* la infraestructura de recolección de información de RCS utiliza una técnica de *proxy-chaining* análoga a los mecanismos de anonimato generalmente utilizados en Tor.[16] En ambos se utilizan varias capas y saltos para evitar la revelación de identidades en el emisor y el destino de los datos.

C. PANORAMA LEGAL EN AMÉRICA LATINA

1. Interceptación de equipos y derechos humanos

La premisa de este informe es que la tecnología tan invasiva y poco regulada del programa Galileo de Hacking Team, pone en peligro no solo el derecho a la privacidad de las comunicaciones en línea, sino también el derecho a la libertad de expresión. Ambos derechos están íntimamente relacionados, pues la vigilancia de este tipo crea un efecto silenciador sobre las expresiones en línea.

En este sentido, la Organización de Estados Americanos (OEA) ha dicho que:

---

[14] Idem

[15] Traducción desde The Intercept: The Hacking Team manuals recommend that customers buy a code signing certificate from Verisign (now Symantec), Thawte, or GoDaddy– companies that offer a stamp of assurance that signals to operating systems and anti-virus scanners that the software is legitimate. Getting what Symantec calls its "digital shrinkwrap" added to Hacking Team software makes it less likely to be detected. (Symantec declined to comment on how it handles malware in issuing certificates. GoDaddy and Thawte did not respond.) https://theintercept.com/2014/10/30/hacking-team/

[16] Idem

> *"5. Resulta preocupante que la legislación en materia de inteligencia y seguridad haya permanecido inadecuada frente a los desarrollos de las nuevas tecnologías en la era digital. Preocupan de manera especial los efectos intimidatorios que el acceso indiscriminado a datos sobre la comunicación de las personas pueda generar sobre la libre expresión del pensamiento, búsqueda y difusión de información en los países de la región."*[17]

Tomando esto en cuenta, la pregunta central de nuestro análisis fue: ¿Es legal este tipo de *software,* no solo en Chile, sino en América Latina? La aproximación a la respuesta fue de dos tipos distintos. Primero un análisis de legalidad de su uso. Y segundo, un análisis de las facultades de las autoridades que compraron el *software.*

Es importante dejar claro que la tecnología de RCS oscila entre la intercepción de comunicaciones y una forma de intrusión a distancia análoga a los allanamientos o pesquisas de lugares físicos por parte de las autoridades. Sin embargo, a diferencia de ambas actividades, las actividades desplegadas por el *software* de Hacking Team no están expresamente reguladas en general, y tampoco existen mecanismos de control sobre el mismo uso. Esto implica una gravedad adicional para el derecho a la privacidad, pues una búsqueda de nuestra computadora, cuentas y redes sociales puede llegar a ser más invasiva que una búsqueda profunda en nuestras casas o recámaras. No existen reglas de control anterior o posterior que nos permitan proteger y exigir nuestros derechos humanos.

Según la OEA, el que no esté regulado es un problema en sí mismo pues si no se establecen límites respecto a la naturaleza, alcance y duración de este tipo de medidas, así como las autoridades facultadas para utilizarlas, se prestan a un uso desproporcionado, y en esa medida, es violatorio de derechos humanos.

> *"8. (…) los Estados deben garantizar que la intervención, recolección y uso de información personal, incluidas todas las limitaciones al derecho de la persona afectada a acceder a información sobre las mismas, estén claramente autorizadas por la ley a fin de proteger a la persona contra interferencias arbitrarias o abusivas en sus intereses*

[17] Relator Especial de las Naciones Unidas (ONU) para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión y Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA. "Declaración Conjunta sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión en Línea." https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=926&lID=2

privados. La ley deberá establecer límites respecto a la naturaleza, alcance y duración de este tipo de medidas, las razones para ordenarlas, las autoridades competentes para autorizar, ejecutar y supervisarlas y los mecanismos legales para su impugnación."

9. Dada la importancia del ejercicio de estos derechos para el sistema democrático, la ley debe autorizar el acceso a las comunicaciones y a datos personales sólo en las circunstancias más excepcionales definidas en la legislación".[18]

Uno antiguo principio legal establece que mientras los ciudadanos podemos hacer todo lo que no esté prohibido, las autoridades solo pueden hacer aquello para lo que están expresamente autorizadas por ley. La lógica es así para poder limitar los abusos de quienes tienen "el monopolio de la violencia legítima", y tener un mecanismo de control sobre las actuaciones de los funcionarios.[19]

2. El contexto legal regional

Si los mecanismos de vigilancia de Hacking Team no estén expresamente regulados en ningún país es problemático en sí mismo pues si las autoridades no tienen facultades expresas para utilizar este tipo de *software.* Por lo tanto, siguiendo los principios de legalidad, proporcionalidad, necesidad e idoneidad reconocidos por el derecho internacional de los derechos humanos, la conclusión sería que los gobiernos no están habilitados para utilizar esta tecnología.

Los alcances de RCS pueden dividirse para ser analizados a partir de tres marcos legales específicos. El primero que se refiere a la interceptación de comunicaciones tanto en el marco de procesos de investigación penal, o en el marco de actividades de organismos de inteligencia en la lucha contra el crimen organizado, el terrorismo y la protección de la "seguridad nacional". En ambos casos, se necesitaría una orden judicial como medida de control para poder justificarlo.

El segundo a las reglas sobre captación de información personal a partir de dispositivos como celulares y computadoras, que idealmente también deberían pasar por controles judiciales para que sean válidas.

---

[18] Idem

[19] Webber, Max. "La Política Como Vocación." *El Político y el Científico*. Madrid: Alianza Editorial, 1919. Página 2.

Por último, las reglas relativas a la inspección de objetos, o bien a las reglas sobre allanamiento o cateo de lugares o moradas, pues en estos últimos suelen establecerse límites específicos que debe contener la orden judicial que los autorice en cuanto a no todas las posesiones de una persona sospechosa pueden ser inspeccionadas. Es decir, que aún en el marco de procesos penales, hay posesiones personales de los acusados que siguen siendo protegidas por las leyes. Si el *software* de Hacking Team por sus capacidades tecnológicas es más invasivo que un allanamiento o inspección física, como mínimo se deberían de respetar estos últimos estándares.

Ciertos países regulan alguno de estos supuestos, mientras ciertos otros han elegido regular realmente poco. En todo caso, todo tipo de invasión que genere el *software* de vigilancia de Hacking Team, que esté fuera de lo regulado en un país en específico, es ilegal. Es decir, que si se regula la intervención de las comunicaciones, pero no la geolocalización o la interceptación de datos de navegación en internet, se puede únicamente realizar la primera conducta y no las otras dos. De lo contrario, se estarían violando derechos humanos tan básicos como los principio de legalidad y seguridad jurídica.

Si a esto le agregamos el uso clandestino y la naturaleza secreta de las actividades de espionaje, se presenta una paradoja adicional pues si bien estas tienen como objetivo preservar los valores de una sociedad democrática, su uso no se rige bajo los parámetros de transparencia y legalidad que forman parte de los mismos.

En América Latina, son pocos los países que no tuvieron contacto con Hacking Team para fines de vigilancia de las comunicaciones, datos e informaciones en línea. Brasil, Chile, Colombia, Ecuador, Honduras, México, Panamá y Venezuela, compraron el programa de la empresa en distintas cantidades y a distintos precios. Adicionalmente, Argentina, Guatemala, Paraguay y Uruguay hicieron negociaciones aunque nunca concretaron la compra.

En América Latina, la empresa más predominante fue Robotec, originaria de Colombia y presente en este país y además con filiales que negociaron dicho *software* en Ecuador y Panamá. En segundo lugar, esta NICE Systems, una empresa israelí presente en Colombia, Honduras y Guatemala. La persona encargada dentro de esta empresa es Ori Zeller: un ex militar israelí que se dedica a la venta de armas AK-47 que eventualmente terminaron en manos de grupos paramilitares de Colombia.[20]

[20] The Interept. “Former AK-47 Dealer Goes Cyber, Supplied Surveillance Tools to Honduras Government”

Una pregunta pendiente, que no es objeto de este informe, es si dichas empresas tendrían algún tipo de responsabilidad internacional solidaria en caso que los programas hayan sido utilizados para espiar a disidentes, periodistas y opositores políticos.

En todos los países analizados, existe el requisito de orden judicial previa a la interceptación de comunicaciones privadas. También encontramos la ilegalidad de las pruebas que se obtengan sin orden judicial o en violación a derechos humanos o al debido proceso. Es decir, que si con el *software* de Hacking Team se obtiene información que puede ser usada para comprobar un delito, pero no existió una orden judicial que autoriza la infección, la prueba debe ser desechada por ser ilegal.

En la región, los límites y modalidades de dicha intervención varían. Por ejemplo, en Brasil solo puede darse para fines de investigación o dentro de procesos penales, se pone como máximo 15 días, y la orden judicial está precedida por la petición de autoridades policiales o el Ministerio Público. En Chile y Colombia, la regla general es que cualquier medida o actividad policial que afecte o ponga en riesgo derechos humanos, debe contar con una orden judicial previa. En Chile además, el máximo es de 60 días e incluye no solo comunicaciones telefónicas, sino de cualquier otro tipo. En Colombia, por otro lado, el límite máximo es de tres meses.

En otros países como Ecuador, el límite es de 90 días salvo en delitos relacionados con delincuencia organizada, en que son seis meses. Si bien se necesita una autorización judicial para intervenir comunicaciones privadas, en este país las mismas están prohibidas si violan derechos humanos de la persona afectada, o si es para el único beneficio político de quien la solicita. Esto llama la atención pues el *software* de Hacking Team habría sido utilizado en Ecuador para espiar a miembros de la oposición política y a disidentes.[21] En Panamá y Argentina también está prohibida la vigilancia de comunicaciones privadas con fines meramente políticos. Los límites en estos países son de 20 y 30 días respectivamente.

---

https://theintercept.com/2015/07/27/ak-47-arms-dealer-goes-cyber-supplied-surveillance-tools-honduras-government/

[21] Según Associated Press, de los correos filtrados surgen pruebas que el gobierno del presidente Rafael Correa utilizó el malware de Hacking Team para espiar a Carlos Figueroa, médico y miembro de la oposición, quien en 2014 fue condenado a seis meses de prisión por "injurias" al presidente después de criticarlo. La evidencia se encontraba en una serie de correos intercambiados entre Luis Solis, funcionario de SENAIN y Bruno Muschitiello de Hacking Team en el que discutían como enviar correos maliciosos que sirvieran como gancho para instalar el software de espionaje en una dirección de correo que coincide con la de "dr.carlosfigueroa." http://bigstory.ap.org/article/6f41d49888174b45857d34511fda1caf/apnewsbreak-email-leak-suggests-ecuador-spied-opposition

En Chile, Honduras, Argentina, Paraguay y Panamá además deben existir sospechas de participación en el delito, o relación con el proceso para que la medida de interceptación de comunicaciones sea aceptada. En varios países, todo lo recolectado que no tenga relación con esto, debe destruirse.

Otra tendencia común es que al hablar de secuestro de correspondencia, o incautación de objetos en el marco de registros domiciliarios, se establecen como límite las comunicaciones entre el acusado y su abogado. En algunos casos como el de Colombia, Ecuador, Honduras, Panamá, Guatemala y Paraguay tampoco se pueden inspeccionar o secuestrar las comunicaciones de las personas que están exentas de testificar, como por ejemplo parejas o aquellas que guardan secretos profesionales sobre las personas investigadas. En otros pocos países, los resultados y diagnósticos médicos también están exentos.

Estos límites son importantes si pensamos en un *software* como el de Hacking Team, pues sus capacidades tan invasivas, y la falta de control sobre el mismo, no discrimina entre comunicaciones protegidas que jamás pueden ser secuestradas o analizadas, como las mencionadas en el párrafo anterior.

Al hablar de la legalidad del *software* de espionaje como el Hacking Team, resaltan tres países que por la amplitud con la que se regula la interceptación de comunicaciones, podrían incluir las prácticas derivadas de dicho programa.

En Colombia se regula de manera muy amplia la interceptación y entrega de la información de tráfico de navegación en internet, y la retención de equipos físicos, virtuales, analógicos o digitales. En estos últimos casos aplican las reglas relativas al allanamiento o registro de domicilios, que están ampliamente regulada en las leyes colombianas. En Ecuador, se permite interceptar datos informáticos, comunicaciones satelitales, móviles, SMS, datos de voz IP y correos electrónicos. Aunque no se regulan límites y excepciones, sí se dice que no puede hacerse violando derechos humanos. La regulación de Panamá, por otro lado, abarca las comunicaciones cibernéticas, los seguimientos satelitales, la vigilancia electrónica y las comunicaciones telefónicas.

Por último, en cuanto a las facultades de los organismos gubernamentales que compraron los programas de Hacking Team, encontramos que ciertas autoridades tienen facultades para interceptar comunicaciones privadas, siempre que exista una orden judicial. Por otro lado, la Policía Nacional de Inteligencia de Colombia, la Senain de Ecuador, la Dirección Nacional de Inteligencia de Honduras, el Cisen de México y la Oficina de Presidencia de Panamá tienen facultades para recabar

inteligencia en el sentido amplio, y no siempre para intervenir comunicaciones. En cualquier caso, el estándar de la orden judicial debe ser respetado.

El caso mexicano es particular en este contexto, pues ocho de las diez autoridades que compraron el *software* de vigilancia, no están facultadas para ejercer este tipo de actividades, y por lo tanto su compra es ilegal.

Detectamos también una tendencia particular en países como Colombia, Ecuador y México: que a pesar de que existen sólidos marcos legales que protegen derechos humanos y regulan la intervención de comunicaciones, en la práctica las actividades de espionaje de estos países son desproporcionadas, y en muchos casos se dirigen a miembros de la oposición política o a activistas y disidentes. Estos tres ejemplos muestran un riesgo creciente en la región: la impunidad y falta de aplicación de la ley, son un factor extra a considerar cuando hablamos de actividades de espionaje en América Latina. Si bien en este reporte se estudia la legalidad de las acciones que pudieran ser abarcadas por el *software* de vigilancia de Hacking Team, eso no es todo, pues en la práctica las actuaciones son contrarias a la legislación. Si a esto se le suma un alto nivel de impunidad, y poca rendición de cuentas, los resultados son distintos.

Debido a los acuerdos internacionales que restringen la exportación de este tipo de tecnologías (como ocurre con el *Arreglo* de *Wassenaar* sobre control de exportaciones de Armas Convencionales y bienes y tecnología de Doble Uso, suscrita también por Italia, el país de la empresa Hacking Team)[22], todos los gobiernos de estos países hicieron contacto con Hacking Team a través de empresas intermediarias.

D. LOS HALLAZGOS EN CHILE

1. Los hechos

En Chile, Jorge Lorca, gerente de la empresa Mipoltec, se contactó con miembros de Hacking Team por primera vez en agosto de 2013.[23] Lorca le escribió a Alex Velasco, gerente regional de Hacking Team, y agendó al menos cuatro reuniones con la Policía de Investigaciones de Chile, Carabineros, el Ejército y la Armada. La relación con la Policía de Investigaciones se formalizó en noviembre de 2014, específicamente a través de su Departamento de Monitoreo Telefónico (Demtel). El

[22] Waassenaar Arrangment. http://www.wassenaar.org/
[23] CIPER, “Los correos que alertaron sobre la compra del poderoso programa espía de la PDI”. http://ciperchile.cl/2015/07/10/los-correos-que-alertaron-sobre-la-compra-del-poderoso-programa-espia-de-la-pdi/

monto total gastado fue de 2,89 millones de euros (sobre 2.285 millones de pesos chilenos).[24]

Originalmente, este organismo no reconoció la compra del *software* de espionaje, pero el día 6 de julio de 2015 emitió un comunicado oficial reconociendo su adquisición. En este último se mencionaba que la vigilancia se hacía con fines estrictamente legales y bajo orden judicial.[25]

Según los correos de Hacking Team,[26] el Departamento de Investigación Electrónica de la Policía de Investigaciones de Chile es el único cliente chileno de HT, aunque existirían más organismos interesados, incluyendo al Ejército y otros departamentos de la misma PDI.[27] La PDI solicitaba software espía principalmente para sistemas Android, utilizando URL maliciosas que redirigen a portales de venta al detalle (como Dafiti, Falabella, Ripley) o de cupones de descuento (Groupon).[28] Es posible deducir que enlaces infectados a esos sitios fueron enviados a las víctimas del software.

2. Legalidad

Legalmente no existe regulación específica sobre este tipo de software, pero como medida intrusiva, debe acogerse al sistema general sobre autorización judicial previa en todo momento: ya sea en investigaciones criminales y procesos penales, o previa la actividad de organismos de inteligencia.

De acuerdo con los artículos 79 y 83 del Código Procesal Penal, la Policía de Investigaciones de Chile no puede interceptar comunicaciones privadas con el *software* de Hacking Team sin que primero el Ministerio Público lo ordene. Esta orden a su vez debe estar basada en una autorización judicial previa que permita su ejecución. El artículo 9 del Código Procesal Penal establece que en la investigación dentro de un proceso penal, si se requiere una medida que vulnere, perturbe o ponga en peligro los derechos fundamentales de los afectados –entre los que se incluye por supuesto el derecho a la privacidad y a la inviolabilidad de las comunicaciones privadas-- debe existir una orden judicial previa.

---

[24] CIPER, “Los correos que alertaron sobre la compra del poderoso programa espía de la PDI”. http://ciperchile.cl/2015/07/10/los-correos-que-alertaron-sobre-la-compra-del-poderoso-programa-espia-de-la-pdi/

[25] La confirmación fue a través de un tuit. Disponible en: https://twitter.com/PDI_CHILE/status/618151545612464128

[26] “Hacking Team, Chile y Ecuador”. https://people.torproject.org/~ilv/ht_chile_ecuador.html

[27] CIPER, “Los correos que alertaron sobre la compra del poderoso programa espía de la PDI”. http://ciperchile.cl/2015/07/10/los-correos-que-alertaron-sobre-la-compra-del-poderoso-programa-espia-de-la-pdi/

[28] “Hacking Team, Chile y Ecuador”. https://people.torproject.org/~ilv/ht_chile_ecuador.html

De manera más específica, el Código Procesal Penal admite y regula la interceptación de comunicaciones en los artículos 222 a 226 si existen sospechas fundadas de que una persona participó en la comisión o en la preparación de un delito. Una vez más, el Ministerio Público es el que está facultado para pedir al juez que ordene la interceptación y grabación de las comunicaciones telefónicas de esta persona, y también se incluyen cualquier "otras formas de telecomunicación." El plazo no puede exceder de 60 días prorrogables.

Por regla, no se pueden interceptar las comunicaciones entre el imputado y su abogado, a menos que el juez de garantía lo ordene. Sin embargo, debemos recordar que la naturaleza del *software* de Hacking Team es tan invasiva que tiene acceso a todo, incluyendo este tipo de correspondencia, sin que existan los mecanismos adecuados para controlarlo.

Como mencionamos previamente, el *software* de Hacking Team es mucho más invasivo que una mera intervención de comunicaciones, pues tiene la capacidad para ver y copiar todo tipo de información, clicks y datos de un dispositivo infectado. En este sentido, el artículo 180 del Código Procesal Penal le da a la fiscalía facultades amplísimas para "llevar a cabo todas las diligencias que considere pertinentes para esclarecer los hechos, tanto realizándolas ellos mismos como poniendo en marcha tales medidas a través de las policías". En principio, esta redacción abre la puerta para que el *software* de Hacking Team sea utilizado --inclusive en relación con personas que no son parte del proceso penal, y en actividades fuera de la interceptación de comunicaciones— con tal de esclarecer los hechos de un caso determinado. En todo caso, aplica la regla general del artículo 9º en lo que respecta a la orden judicial previa como requisito para cualquier diligencia que sea capaz de afectar derechos fundamentales.

En esta misma capacidad invasiva, podría establecerse una relación análoga entre la infección del *Remote Control System* y la incautación de una computadora o un teléfono celular. Si bien no es una "incautación física" ni una sustracción de objetos, el efecto es el mismo pues permite analizar ciertos elementos que pudieran tener valor probatorio. El artículo 197 del Código Procesal Penal establece las reglas para la incautación de objetos, documentos o instrumentos que "parecieren haber servido o haber estado destinados a la comisión del hecho investigado (…) o los que pudieren servir como medios de prueba".

En otro rubro, en cuanto a la interceptación de comunicaciones realizada por agencias de inteligencia, se debe igualmente respetar los derechos humanos en las

gestiones investigativas destinadas a obtener pruebas. Sin embargo, varía su regulación en cuanto a los requisitos de procedencia y la amplitud de las medidas de recolección de información que pueden llevarse a cabo.

Radicalmente distinto es el panorama en el ámbito de la recolección de información con fines de inteligencia. El artículo 24 de la Ley 19.974 sobre el Sistema de Inteligencia del Estado y que crea la Agencia Nacional de Inteligencia (ANI), establece que con el fin de enfrentar riesgos para la seguridad nacional como el terrorismo y el narcotráfico, pueden realizarse procedimientos especiales de obtención de información:

> 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.

Dado lo amplia de la redacción, el uso del *software* de Hacking Team estaría respaldado por este artículo, particularmente en sus literales b) y d). No se trata de un intento de la legislación por cubrir el uso de *malware* por parte del Estado, sino de reglas fijadas hace más de diez años, que ante el cambio de contexto y los avances de la tecnología se han vuelto problemáticas desde la perspectiva de su adecuación a un esquema de respeto a los derechos humanos.

La capacidad operativa para ejecutar las acciones de recolección de información con fines de inteligencia está radicada en las direcciones de inteligencia de las fuerzas armadas y de orden, y es a ellas que se autoriza la actuación por parte de un miembro de la Corte de Apelaciones de la jurisdicción donde se ejecute la medida (artículo 25 de la Ley 19.974).

Puesto que fue la Policía de Investigaciones de Chile quien compró el programa, su utilización dentro del marco de la inteligencia estatal estaría sujeta a tales reglas. Esto implica un bajo nivel de transparencia en el uso de la información: por tratarse de trabajo de recolección de información con fines de inteligencia, los antecedentes de tales labores están sujetos a reserva (artículo 38 de la Ley 19.974). Dicha obligación de secreto se extiende a los funcionarios estatales (como los tribunales o miembros del Congreso) encargados del control de la actividad de inteligencia que solicitaren información sobre dichas operaciones (artículo 39) y a quienes sin ser funcionarios de los organismos de inteligencia, tomaren conocimiento de las

solicitudes para la ejecución de procedimientos especiales de obtención de información, sus antecedentes o las resoluciones judiciales respectivas (artículo 40).

Común a los sistemas procesal penal y de recolección de información con fines de inteligencia es la falta de un deber de notificación a las personas sujetas a una investigación no formalizada, es decir, de aquella investigación donde no se ha procedido a comunicar a una persona sobre la investigación de delitos en su contra. El artículo 224 del Código Procesal Penal obliga a comunicar al afectado por la interceptación de telecomunicaciones "con posterioridad" a la medida y mientras la investigación lo permitiere y no signifique riesgo para terceros, sin resguardos afines para otras formas de afectación no detectada de derechos fundamentales. Si dentro de ese proceso se usó software malicioso, podría no ser comunicado jamás. De este modo, una persona podría nunca enterarse que está siendo objeto de una intervención de sus equipos, sino en la medida en que pueda detectar la existencia del *malware* de Hacking Team.

En principio, si con el *software* de Hacking Team se obtiene información que podría resultar útil como prueba en un juicio y no se siguen las reglas previamente especificadas, la misma debe ser desestimada de acuerdo con el artículo 276 del Código Procesal Penal. Es decir, que cualquier cosa que se encuentre en la computadora o teléfono infectado, no puede servir para culpar a una persona si no se siguen las reglas procesales adecuadas.

En suma, solo podría usarse una herramienta tecnológica de tal calibre en los casos en que un juez lo permita a petición del propio Ministerio Público o los organismos de inteligencia. Por lo mismo, no se puede hacer de manera masiva, sino con un uso acotado, dentro de un procedimiento o en investigaciones de los aparatos de inteligencia del país, respetando siempre los requisitos legales de procedencia y el marco de actuación autorizado (tanto respecto de quienes serán afectados por estas diligencias como por la materia que se quiere averiguar con ellas).

No obstante, de lo anterior no se concluye que el uso de herramientas tales como las ofrecidas por Hacking Team y adquiridas por la PDI esté cubierto por el ordenamiento jurídico chileno. Una comprensión cabal del sistema normativo no puede obviar la existencia de normas de rango constitucional que consagran derechos fundamentales, que pueden verse afectados en su esencia, aun con la aparente venia del texto de la ley o por el cumplimiento de requisitos de justicia formal. Una posible sanción judicial a partir de información recogida mediante esta clase de software podría significar una lesión al debido proceso, desde la

presunción de inocencia hasta el derecho a la inviolabilidad de las comunicaciones privadas.

Por último, si no se respetan estos requisitos previamente mencionados, la Ley de Delitos Informáticos podría ser aplicada al funcionario público que utilice el *software* de Hacking Team sin la debida autorización judicial, y por un tiempo indeterminado si "con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él". Esto último se castiga con cárcel.

En el caso particular del uso de la información adquirida dentro de los supuestos de la recolección de información con fines de inteligencia, el funcionario que utilizare la información recopilada o elaborada por dichos organismos en beneficio propio o ajeno, en perjuicio de alguna persona, autoridad u organismo, o para ejercer presiones o amenazas, será sancionado con la pena de reclusión mayor en sus grados mínimo a máximo y la inhabilitación absoluta y perpetua para ejercer cargos públicos.

F. CONCLUSIONES Y RECOMENDACIONES DE POLÍTICA PÚBLICA

En América Latina, las actividades de vigilancia y espionaje gubernamental son problemáticas si tomamos en cuenta el historial de autoritarismos y represiones en la región. Frente a instituciones democráticas débiles y deficiencias en la aplicación de la ley, programas de espionaje tan invasivos como el de Hacking Team se prestan a abusos y violaciones a derechos humanos. En la región –y no siempre-- suelen regularse las acciones y consecuencias de la interceptación de comunicaciones o correspondencia, incautación de equipos, geolocalización y registros domiciliarios pero no se regula el código.

El objetivo principal de los sistemas de investigación criminal y de inteligencia es salvaguardar la seguridad, la paz y los principios de cada país. Sin embargo y de manera paradójica, estos objetivos se logran mediante mecanismos secretos con poca rendición pública disponible cuando precisamente, por el objetivo democrático que persiguen, deben ser objeto de controles ciudadanos y rendición de cuentas.

Lo anterior no parece verificarse en el caso de Hacking Team. Esto responde a varias razones: políticas, históricas, legales y prácticas, que hacen difícil un control sobre la actividad estatal de investigación y vigilancia. Si bien es importante realizar modificaciones legales con miras al resguardo de intereses fundamentales, también

es necesario que exista una cultura de transparencia y respeto de derechos humanos que, dentro del marco vigente, sepa poner a los derechos fundamentales de las personas, consideradas de forma individual y colectiva, en el centro de la función de recolección de información.

La vigilancia de las comunicaciones privadas interfiere con el derecho a la intimidad, a la libertad de expresión y pensamiento y opinión. Como resultado, solo puede estar justificada cuando es prescrita por ley, es necesaria para lograr un objetivo legítimo, y es proporcional al objetivo perseguido. Asimismo, mecanismos de transparencia y rendición de cuentas permiten un control externo sobre una capacidad con alto riesgo de daño en caso de abuso.[29]

La vigilancia dirigida puede ser necesaria, pero no puede utilizarse de manera arbitraria porque entonces los funcionarios y gobiernos que la utilizan estarían cayendo en lo mismo que buscan erradicar. Debe existir leyes claras y mecanismos de control para prevenir abusos, tanto internos como externos.

Si bien la vigilancia puede ejercerse de manera legítima con objetivos claros, se deben delimitar conceptos de “seguridad nacional” y “orden público” para que los mismos no sean abusados en el marco de actividades de espionaje. Su aplicación deberá autorizarse únicamente cuando exista un riesgo cierto respecto de los intereses protegidos y cuando ese daño sea superior al interés general de la sociedad en función de mantener el derecho a la privacidad y a la libre expresión del pensamiento y circulación de información. Esto implica la necesidad de que existan mecanismos para controlar que las atribuciones legales no sean abusadas con propósitos ilegítimos.[30]

Cuando hablamos sobre *software* como el de Hacking Team es necesario impedir que los gobiernos tengan acceso y guarden “zero days”. Todo tipo de vulnerabilidad en aplicaciones debe ser transparentado para que no se preste a futuros abusos. Una regulación en materia de ciberseguridad sensible a esta clase de desarrollos debe ser considerada por el Estado.

Las leyes deben proteger a los informantes o *whistleblowers* para no sancionar a personas vinculadas al Estado, que teniendo la obligación legal de mantener confidencialidad sobre cierta información, divulguen información de interés público.

---

[29] Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. https://es.necessaryandproportionate.org/text

[30] La Relatoría Especial expresa preocupación ante la adquisición e implementación de programas de vigilancia por parte de Estados del hemisferio https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=998&IID=2

La exención de responsabilidad debe extenderse asimismo a los medios que hagan públicas las revelaciones obtenidas por esta clase de fuentes.

Las decisiones de realizar tareas de vigilancia que invadan la privacidad de las personas deben ser autorizadas por autoridades judiciales imparciales e independientes. Idealmente, estas deben estar separadas de las autoridades que encargadas de la vigilancia de comunicaciones, y correctamente capacitadas para ejercerlas.[31] Por la complejidad del tema, a veces los jueces no saben qué están autorizando, ni los posibles riesgos que los programas de vigilancia podrían traer. Para evaluar la autorización de las medidas, los jueces deben seguir los criterios de debido proceso y los principios de necesidad, idoneidad y proporcionalidad.[32]

Estos controles judiciales deben ser ex ante y autorizar las medidas invasivas, pero pero también ex post en caso que se violen derechos humanos. Es decir, se deben establecer garantías suficientes para que las personas afectadas puedan impugnar posibles excesos en esta área como en cualquiera otra en que sus derechos hubieren sido violados. Entre estas garantías está la de notificación al usuario que les permita tener tiempo y la información suficiente para que puedan impugnar la decisión o buscar otras soluciones.[33] Se necesitan mecanismos de transparencia y rendición de cuentas que traigan aparejado un cumplimiento cabal del derecho de acceso a la información en relación con la actividad del estado respecto de una persona, en el que las excepciones y los límites al acceso estén fuertemente acotados. Debe exigirse la desclasificación de informes después de cierto período y destrucción de información recolectada.

Por último, la OEA ha señalado que la vigilancia de las comunicaciones y las injerencias a la privacidad que excedan lo estipulado en la ley, que se orienten a finalidades distintas a las autorizadas por ésta o las que se realicen de manera clandestina deben ser sancionadas.[34] Esto incluye la vigilancia realizada por motivos políticos contra defensores de derechos humanos, periodistas y opositores políticos. Por otro lado, el Estado tiene la obligación de divulgar ampliamente la información sobre programas ilegales de vigilancia de comunicaciones privadas e informar a las víctimas de los mismos.

---

[31] Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones https://es.necessaryandproportionate.org/text

[32] Idem

[33] Idem

[34] La Relatoría Especial expresa preoc¯upación ante la adquisición e implementación de programas de vigilancia por parte de Estados del hemisferio
https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=998&IID=2

Cada juez y agencia de inteligencia así como las instituciones de las que dependen, deben tener mecanismos claros de actuación dentro sus parámetros internos. Los servicios de inteligencia, que en toda la región tienen facultades más amplias para ejercer este tipo de espionaje, deben actuar en el marco de un reglamento que especifique controles y responsabilidades claras; facultades bien establecidas y tipos de tecnología aplicables. Por otro lado, se deben transparentar y discutir los criterios para decidir quiénes son los “sospechosos” o posibles infectados. En cada caso, los parámetros son distintos, y no deben implicar criterios discriminatorios por razón de edad, raza, religión, género o posición política.