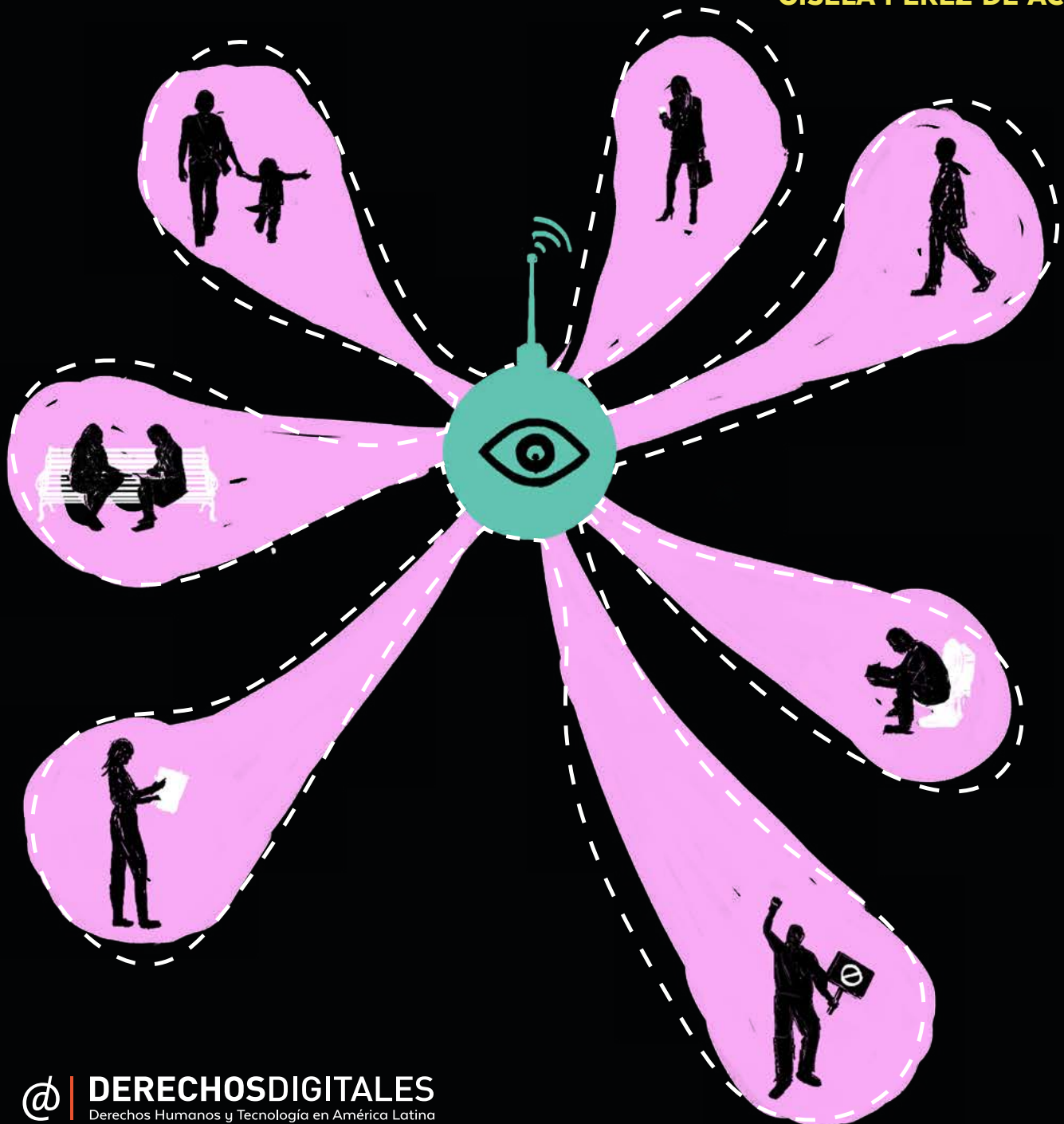


INFORME:

HACKING TEAM MALWARE PARA LA VIGILANCIA EN AMÉRICA LATINA

GI SELA PÉREZ DE ACHA



INFORME:

HACKING TEAM MALWARE PARA LA VIGILANCIA EN AMÉRICA LATINA

GI SELA PÉREZ DE ACHA

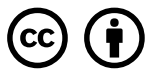
Derechos Digitales:

Organización No Gubernamental fundada en el año 2005, 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 están la libertad de expresión, los derechos de autor y la privacidad.

Diseño y diagramación: Constanza Figueroa

Corrección: Vladimir Garay

Marzo de 2016



Esta obra está disponible bajo licencia Creative Commons
Attribution 4.0 Internacional (CC BY 4.0):
<https://creativecommons.org/licenses/by/4.0/deed.es>

Agradecimientos

Agradecemos a las siguientes personas y organizaciones por su colaboración en este reporte:

Andrés Delgado - Apertura Radical

Edy Alexander Tábor

Israel Leiva- Derechos Digitales

Larissa Ribeiro y Joana Varon - Coding Rights

Leandro Ucciferri - Asociación por los Derechos Civiles

Lia Patricia Hernández - IPANDETEC

Marianne Díaz Hernández - Acceso Libre

Maricarmen Sequera - TEDIC

Matías Jackson

Natalia Zuazo

Renata Ávila - The World Wide Web Foundation

Valentina Hernández - Derechos Digitales

El equipo de Fundación Karisma

Contenidos

Hacking Team: el negocio de espiar a las personas	6
Resumen ejecutivo	7
1. Introducción	9
2. Tecnología	12
¿En qué dispositivos funciona?	12
¿Cómo se instala?	12
¿Qué hace el software con el equipo infectado?	13
¿Quién lo opera?	14
¿Cuál es su funcionamiento técnico?	14
Figura 1: ¿Cómo funciona Remote Control System?	15
¿Por qué es indetectable?	16
3. Panorama legal en américa latina	18
3.1. Interceptación de equipos y derechos humanos	18
3.2. Adquisición estatal de malware para la vigilancia de comunicaciones	20
3.3. Regímenes legales de investigación mediante medidas intrusivas	21
4. Clientes de Hacking Team en América Latina	24
4.1. Brasil	24
4.2. Chile	28
4.3. Colombia	32
4.4. Ecuador	37
4.5. Honduras	41
4.6. México	43
4.7. Panamá	48
5. Otros países que negociaron con Hacking Team	53
5.1. Argentina	53
5.2. Guatemala	59
5.3. Paraguay	63
5.4. Uruguay	66
5.5. Venezuela	68
6. Conclusiones generales	71
Bibliografía	75

HACKING TEAM EN AMÉRICA LATINA



Hacking Team, una de las empresas más importantes en el rubro del software de vigilancia, fue hackeada y sus negocios en América Latina fueron expuestos.



¿Compró tu gobierno tecnología para espiar a sus ciudadanos? ¿Qué agencias estatales adquirieron sus productos? ¿Cuánto gastaron? ¿Están vigilando activistas y disidentes políticos?



* Información basada en la filtración del 5 de julio del 2015.

** Bolivia planeó reunirse con Hacking Team, pero no hay información respecto a si la reunión se llevó a cabo.

QUE LA SEGURIDAD NO SEA USADA COMO EXCUSA PARA VIOLAR DERECHOS HUMANOS



¡LA PRIVACIDAD ES UN DERECHO!



Resumen ejecutivo

Creciente es el interés en el espionaje digital por parte de los gobiernos de América Latina. Esta es una de las conclusiones de “Hacking Team: malware de espionaje en América Latina”, un nuevo informe realizado por Derechos Digitales y que revela que la gran mayoría de los países de la región estuvieron involucrados con Hacking Team, la cuestionada empresa italiana creadora de Remote Control System (RCS), un software espía que se vende a organizaciones gubernamentales alrededor del mundo.

Brasil, Chile, Colombia, Ecuador, Honduras, México y Panamá compraron licencias para el uso de Galileo o DaVinci, los nombres comerciales de RCS. Argentina, Guatemala, Paraguay, Perú, Uruguay y Venezuela contactaron a la empresa y negociaron precios, pero no hay información respecto a si las ventas fueron concretadas.

Las compras y negociaciones se hicieron través de empresas intermediarias. Las más recurrentes fueron Robotec, en Colombia, Ecuador y Panamá, y NICE Systems, en Colombia, Honduras y Guatemala.

Las negociaciones se realizaron en secreto, hasta que el 5 de julio de 2015 se expusieron públicamente 400 GB de información de la empresa, incluyendo correos electrónicos, facturas, documentación interna y parte del código de Hacking Team.

RCS es un software capaz de acceder a cualquier tipo de información contenida en una computadora o teléfono celular: contraseñas, mensajes y correos electrónicos, contactos, llamadas y audios de teléfono, micrófono y webcam, información de herramientas como Skype y otras plataformas de chat, posición geográfica en tiempo real, información almacenada en el disco duro, cada una de las teclas apretadas y clics del mouse, capturas de pantalla y sitios de internet visitados, y más. En otras palabras, prácticamente todo lo que transcurre en un equipo personal.

Del análisis de las normas vigentes en cada uno de los países que se relacionaron con Hacking Team, así como de las notas de prensa que surgieron en la región a tras las revelaciones, el informe concluye que el software de Hacking Team es contrario a los estándares legales de cada país, y además violatorio de los derechos a la privacidad, a la libertad de expresión y al debido proceso. Considerando la relación cercana que nuestra región tiene con el autoritarismo, es especialmente preocupante que las autoridades cuenten con herramientas de este tipo.

En Ecuador se utilizó tecnología de Hacking Team para vigilar a Carlos Figueroa, opositor del gobierno de Rafael Correa. En México, un país que vive una seria crisis de derechos humanos, ocho de las diez autoridades que compraron RCS no están facultadas para ejercer actividades de vigilancia; El Centro de Investigación y Seguridad Nacional (CISEN), un organismo de inteligencia, realizó 2,074 órdenes judiciales para poder utilizar el software; hasta la fecha, no se sabe si su uso es justificado.

La filtración también reveló que de la información de Hacking Team permitió saber que la

Drug Enforcement Agency (DEA) de Estados Unidos intercepta todas las comunicaciones de todos los ciudadanos colombianos. Así mismo, se sospecha del uso de herramientas de este tipo contra Vicky Dávila, periodista que investiga una red de prostitución masculina al interior de la policía.

En Panamá, el ex presidente Ricardo Martinelli estuvo personalmente al tanto de las negociaciones con Hacking Team. En Chile, en cambio, la Policía de Investigaciones dijo en un comunicado que la vigilancia se hacía con fines estrictamente legales y bajo orden judicial. Sin embargo, las órdenes judiciales en este caso no son suficientes para garantizar el uso legítimo del software de espionaje.

En términos legales, este tipo de software no está regulado explícitamente en ningún país. En México y Colombia existen disposiciones amplias al respecto, pero con lenguaje vago e impreciso. La ausencia de regulación deja al arbitrio de las autoridades, muchas veces corruptos, el uso, aplicación y objetivos de RCS.

Si bien la interceptación de comunicaciones bajo orden judicial está regulada en todos los países, con mayores o menores salvaguardas, esta no es suficiente pues el software de Hacking Team es mucho más invasivo que una mera interceptación: abarca el acceso a documentos, webcam, disco duro, teclado y geolocalización de los equipos afectados. Como esto no es parte de la legislación, dudosamente es parte del orden judicial, por lo que el derecho al debido proceso también se ve vulnerado.

Cabe resaltar que en casi todos los países analizados existen sanciones penales contra quien invada o intervenga los sistemas informáticos o las comunicaciones privadas de una persona fuera de la legalidad de una investigación. Sin embargo, sólo Panamá ha abierto procesos al respecto.

El problema del espionaje indebido va mucho más allá de Hacking Team, implica a un mercado global que abusa la tecnología de vigilancia en manos de gobiernos alrededor del mundo. En este sentido debe existir mayor transparencia en el uso y adquisición de estas herramienta, una discusión abierta sobre los estándares que deben regir esta tecnología y además sanciones penales en los casos que lo ameriten.

1. Introducción

Software para perseguir delitos, aunque en su operación se cometan delitos. *Malware* para preservar la seguridad, con secretismo y opacidad. Vulneración intencional de sistemas informáticos para hacer cumplir la ley, aprovechando los vacíos regulatorios de la misma. Esa es la lógica detrás de los productos de Hacking Team, la empresa italiana encargada de vender y comercializar algunos de los programas computacionales de vigilancia más invasivos que se conocen en el mundo. Con venta únicamente a gobiernos, su mensaje publicitario es 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 son algunos de los nombres comerciales con que se conoce a Remote Control System (RCS), programa de monitoreo de comunicaciones creado con un objetivo legítimo: combatir la delincuencia. La traducción literal de RCS, “Sistema de Control Remoto”, revela el funcionamiento del programa: una vez que los dispositivos son inoculados, pueden ser controlados a distancia. Lo que distingue a RCS con el resto de formas de vigilancia tradicionales –como las escuchas telefónicas– es que no solo tiene acceso a conversaciones y comunicaciones, sino que puede capturar todo tipo de información, imágenes y datos que se encuentren en las computadoras o celulares afectados, sin que sea necesario que los mismos viajen por internet.² Es decir, no interviene comunicaciones únicamente, tiene acceso a datos estáticos en los dispositivos.

RCS incluso 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, puede activar cámaras y micrófonos.

Hasta ahora, por la naturaleza secreta de las actividades de espionaje, poco sabíamos de qué trataba este *software*, cuáles eran sus alcances y posibles daños. Pero eso cambió cuando el domingo 5 de julio de 2015 se expusieron públicamente 400 GB de información de Hacking Team. Los documentos incluían facturas, correos electrónicos, datos fiscales y código fuente, entre otros archivos.³

1 Manish Singh. “Hacking Team, Boeing Worked on Drones That Infect Computers Over Wi-Fi”. Gadgets 360° 23 de julio de 2015. Consultado el 19 de agosto de 2015. <http://gadgets.ndtv.com/internet/news/hacking-team-boeing-worked-on-drones-that-infect-computers-over-wi-fi-719033> (Traducción de la autora)

2 Bill Marczak, Claudio Guarnieri, Morgan Marqui S - Boire, y John Scott - Railton. “Mapping Hacking Team’s ‘Untraceable’ Spyware”. Munk School of Global Affairs, 14 de febrero de 2014, 1-9. Consultado el 8 de noviembre de 2015. <https://citizenlab.org/wp-content/uploads/2015/03/Mapping-Hacking-Team’s-‘Untraceable’-Spyware.pdf>.

3 Steve Ragan. “Hacking Team Hacked, Attackers Claim 400GB in Dumped Data”. CSO. 5 de julio de 2015.

Con la filtración supimos que seis países de América Latina son clientes de Hacking Team: Brasil, Chile, Colombia, Ecuador, Honduras, México y Panamá. Otros países como Argentina, Guatemala, Paraguay, Uruguay y Venezuela también negociaron con la empresa, pero no concretaron la compra, al menos dentro del período de tiempo cubierto por la filtración.

Hacking Team sustenta la venta de sus productos en la supuesta legalidad de los mismos, en su propósito de combate al crimen y en el rechazo al abuso de sus capacidades. En sus términos y condiciones, la empresa se jacta de no vender *software* a países que “facilitan graves violaciones a derechos humanos”. Sin embargo, está comprobado que RCS se usa para espiar a disidentes políticos, periodistas y defensores de derechos humanos.⁴

Tres de los clientes de Hacking Team –Uzbekistan, Arabia Saudita y Sudán– están entre los peores países en términos de libertades, según el índice Freedom House 2015.⁵ Otros tres clientes –Colombia, México y Turquía– están listados por el Comité para la Protección de Periodistas entre los veinte países más peligrosos en el mundo para el ejercicio de la profesión.⁶

Llama la atención que la empresa siga operando.⁷ A pesar de la filtración y la publicación de los contratos entre Hacking Team y distintos organismos gubernamentales, en ningún país se han abierto investigaciones al respecto.

El análisis de las legislaciones de los países latinoamericanos que negociaron con Hacking Team demuestra que no existen regulaciones específicas para Galileo o DaVinci, o bien, que las reglas existentes no son plenamente aplicables. Por lo mismo, la adquisición y uso de este tipo de programas exige una discusión abierta sobre los estándares legales deben regir este tipo de tecnología, tanto respecto de su adquisición como de su operación.

Por el historial de autoritarismos y violaciones a derechos humanos en América Latina, surgen interrogantes: ¿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?

No se trata de preguntas sobre una empresa en particular o un programa computacional específico. Las revelaciones sobre Hacking Team dieron cuenta de un mercado en el que participan múltiples actores a nivel global, donde se transan altísimas cantidades de dinero y donde el producto tiene un fuerte potencial para el abuso y la violación de derechos fun-

Consultado el 8 de octubre de 2015. <http://www.csoonline.com/article/2943968/data-breach/hacking-team-hacked-attackers-claim-400gb-in-dumped-data.html>

4 Privacy International. “Briefing for the Italian Government on Hacking Team”. Abril y mayo de 2015. Consultado el 19 de septiembre de 2015. <https://privacyinternational.atavist.com/hackingteamsurveillanceexports>.

5 Ídem

6 Ídem

7 Sus servicios pueden consultarse y contratarse en la página oficial <http://www.hackingteam.it/>

damentales. Hacking Team se convierte así en un caso de estudio para un asunto mayor: la adquisición, el uso y el abuso de capacidades tecnológicas altamente invasivas por gobiernos de Latinoamérica y la falta de mecanismos de control.

Al no estar expresamente regulado el apoderamiento remoto de equipos, y por ser altamente intrusivo como procedimiento, el uso del *software* de espionaje que vende la empresa es contrario a los derechos humanos. En la mayoría de los casos estudiados se exige una orden judicial para poder interceptar comunicaciones; ya que las capacidades de RCS exceden por lejos la mera interceptación, tendría que existir una orden judicial para cada geolocalización, activación de micrófono o cámara, e inspección de portapapeles, y otra para intervenir las comunicaciones. Su uso aprovecha un vacío en la regulación de las interceptaciones pasivas de comunicaciones y las pesquisas o búsquedas físicas.

Por lo mismo, cabe explorar la legalidad aplicable y si su operación amerita una sanción en cada uno de los países estudiados.

En este documento analizaremos los componentes técnicos del *software* de Hacking Team para saber cómo se instala, con qué criterios, a quiénes y qué implicaciones o peligros se presentan. Luego compilamos todos los hechos relativos a Hacking Team en los países de América Latina, para finalmente hacer un análisis legal en cuanto a las facultades y el debido proceso en cada país. Como veremos, cuando la tecnología de vigilancia no está expresamente regulada, se abre la puerta para que viejas prácticas autoritarias se instalen en la región y operen al margen de la ley.

2. Tecnología

Para entender cómo funciona Remote Control System revisamos los manuales de uso de la empresa, publicados por *The Intercept* en octubre de 2014.⁸ En ellos, Hacking Team detalla instrucciones minuciosas para los técnicos, administradores y analistas sobre cómo inocular un dispositivo y echar a andar los mecanismos de espionaje.

¿En qué dispositivos funciona?

A través de alguno de los métodos que se señalan a continuación, el *software* de espionaje puede implementarse en cualquier computadora con OS X (en equipos Apple), Microsoft Windows o GNU/Linux. También en cualquier teléfono móvil inteligente o tableta con sistema operativo Android, BlackBerry, iOS (iPhone), Symbian o Windows Mobile.⁹

¿Cómo se instala?

El *software* puede instalarse de varias formas. Cada una es efectiva en 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 “engaño” a la persona afectada. Es decir, aunque no se requiera de la interceptación directa de la víctima, siempre aparenta ser algo distinto y se “esconde” para poder instalarse. Distintas vías pueden utilizarse para ese resultado.

La primera forma en que puede instalarse es de manera física a través de una llave USB o usando un equipo especial llamado *Tactical Network Injector*, siempre y cuando las autoridades tengan acceso directo a la computadora. Por ejemplo, en un retén policial o cateos en aeropuertos.¹⁰

La segunda forma es mediante la emulación de una red de conexión inalámbrica a internet (*Wi-Fi*) para ganar acceso a la computadora mediante un falso punto de conexión a internet ofreciéndose a quien requiera acceso a la red. También se puede vulnerar la clave de una red *Wi-Fi* existente para infiltrarse en ella. Para generar la señal, el adversario espera en un lugar cercano al equipo, como el lobby de un hotel o un café donde se encuentre la víctima.¹¹

La tercera forma es utilizando vías remotas o “no-físicas”. El tipo más común es una falsa invitación por correo electrónico para poder instalar el *software* de RCS. Eso pasó con el opositor al Gobierno de Rafael Correa en Ecuador, Carlos Figueroa, a quien enviaron un correo con un enlace de invitación a un evento inexistente para poder infectar su computadora.¹² En el

8 Corra Currier y Morgan Marquis-Boire. “Secret Manuals Show the Spyware Sold to Despots and Cops Worldwide”. *The Intercept*. 30 de octubre de 2013. Consultado el 8 de noviembre de 2015. <https://theintercept.com/2014/10/30/hacking-team/>

9 Ídem

10 Ídem

11 Ídem

12 Ver apartado referido a Ecuador, en este mismo informe.

caso de periodistas, por ejemplo, se les envía correos con adjuntos que prometen información exclusiva. Una vez que lo abren se instala el programa malicioso.¹³

Adicionalmente, el *software* se puede esconder en descargas legítimas de aplicaciones en celulares.¹⁴ También son comunes los envíos de mensajes de texto con enlaces a falsas promociones y descuentos que, una vez que se abren, instalan *malware* en el equipo.¹⁵

Un enlace así puede esconderse en cualquier tipo de tráfico no cifrado en internet, por ejemplo streaming en videos de Youtube o Microsoft Live. Para esto se utiliza un equipo especial (llamado Network Injector Appliance) que se instala directamente a través de las empresas proveedoras de servicio y que, dependiendo de los patrones de tráfico, permite inocular a múltiples usuarios al mismo tiempo. Este método no requiere interceptación directa del usuario: basta con que se haga uso de internet en el día a día.¹⁶

El uso de “*exploits*” es común en casi todos los métodos. Estos se aprovechan de los errores (*bugs*) y vulnerabilidades en sistemas computacionales¹⁷ con el propósito de introducir programas o funciones no consentidas por el usuario. En esta categoría, Hacking Team ofrece la posibilidad de usar un tipo de *exploit* bastante controversial: los códigos maliciosos secretos o no revelados (*zero-day*) que aprovechan fallos de *software* no conocidos públicamente y que, por ende, no han sido comunicados a su desarrollador ni consecuentemente reparados. De ahí que se les llame “de día cero”, en función de que no ha existido tiempo de reacción entre el descubrimiento de la vulnerabilidad y la adopción de alguna medida que se haga cargo de ella.

¿Qué hace el *software* con el equipo infectado?

Una vez inoculado un ordenador o un teléfono, el operador remoto (o “analista”) puede acceder y copiar desde el mismo equipo cualquier tipo de información contenida. El manual lista lo siguiente: contactos, aplicaciones utilizadas, calendario, llamadas y audios de teléfono, Skype, cámara y webcam, chat, todo lo copiado al portapapeles, archivos abiertos por la víctima, disco duro, teclas apretadas, mensajes y correos electrónicos, micrófono y audio, clics del *mouse*, contraseñas, posición geográfica en tiempo real, impresiones, cap-

13 Frank Bajak. “South America Hacker Team Targets Dissidents, Journalists”. The Big Story. 9 de diciembre de 2015. Consultado el 8 de marzo de 2016. <http://bigstory.ap.org/article/fa7618cf36a642fb900a4f35b2c986b1/south-america-hacker-team-targets-dissidents-journalists>

14 Morgan Marquis-Boire, John Scott - Railton, Claudio Guarnieri, y Katie Kleemola. “Police Story: Hacking Team’s Government Surveillance *Malware*”. Munk School of Global Affairs, Junio 2014, 2-25. Consultado el 23 de septiembre de 2015. <https://citizenlab.org/wp-content/uploads/2015/03/Police-Story-Hacking-Team’s-Government-Surveillance-Malware.pdf>

15 Ibidem, The Intercept. Octubre 2013

16 Después de que The Intercept reveló esta falla en los sistemas de YouTube y Microsoft Live, ambas compañías tomaron medidas para disminuir el riesgo. Ver Morgan Marquis-Boire. “You Can Get Hacked Just By Watching This Cat Video on YouTube”. The Intercept. 15 de agosto de 2015. Consultado el 25 de agosto de 2015. <https://theintercept.com/2014/08/15/cat-video-hack/>

17 Ibidem, Munk School of Global Affairs. Junio de 2014.

turas de pantalla y sitios de internet visitados.¹⁸ Además, puede tener acceso a los archivos locales de redes sociales y aplicaciones de chat, incluyendo Facebook, Viber, WhatsApp, LINE y QQ.¹⁹ En otras palabras, permite acceso a prácticamente todo lo que transcurre en un equipo personal.

Una vez que se tiene acceso, el programa rastrea los vínculos, lugares y personas que tienen relación con de la víctima, en función de la constancia del contacto que tengan con ella.²⁰

¿Quién lo opera?

En principio, los operadores son siempre funcionarios de organismos gubernamentales capacitados por Hacking Team. Quienes operan el espionaje personalizado día a día son llamados “analistas” y se encargan de obtener y analizar la información recopilada de las víctimas inoculadas. Esto incluye la vinculación entre la recopilación de información mediante el *malware* y labores de inteligencia para descubrir nexos y conexiones entre distintos tipos de individuos. Por otro lado, quienes realizan la instalación de nuevos programas son llamados “técnicos” y se encargan de solicitar la creación de nuevo *software* espía, dependiendo del método y sistema operativo a infectar.

A pesar de que el manual señala que esto último puede ser realizado de manera autónoma, en los correos filtrados se puede apreciar que existe una constante comunicación entre los funcionarios gubernamentales de países compradores y los ingenieros de Hacking Team para solicitar la creación de nuevas soluciones de espionaje.²¹

¿Cuál es su funcionamiento técnico?

La Figura 1 muestra el funcionamiento técnico de Remote Control System, donde se pueden apreciar tres partes fundamentales:

1) Red interna de RCS. Manejada por los organismos gubernamentales que compraron el *software* de espionaje y sus agentes. Posee un único punto de acceso pú-

18 Corra Courier, y Morgan Marquis-Boire. “Secret Manuals Show the Spyware Sold to Despots and Cops Worldwide”. The Intercept. 30 de octubre de 2014. Consultado el 8 de febrero de 2016. <https://theintercept.com/2014/10/30/hacking-team/#manuals>.

19 Ídem

20 Después de la filtración se generaron también dudas sobre la capacidad que RCS tenía para implantar información dentro de los equipos infectados por una línea de código que permitía introducir pornografía infantil. Ver “RCS-Common Evidence”. Github. 23 de mayo de 2014. Consultado el 3 de marzo de 2016 <https://github.com/hackedteam/rcs-common/blob/master/lib/rcs-common/evidence/file.rb#L17>. No obstante, la información fue desmentida Graeme Burton. “Did Hacking Team design software that could plant child porn on suspects’ PCs?” Computing. 6 de Julio de 2015. Consultado el 5 de marzo de 2016. <http://www.computing.co.uk/ctg/news/2416521/did-hacking-team-sell-software-to-plant-child-porn-on-suspects-pcs>

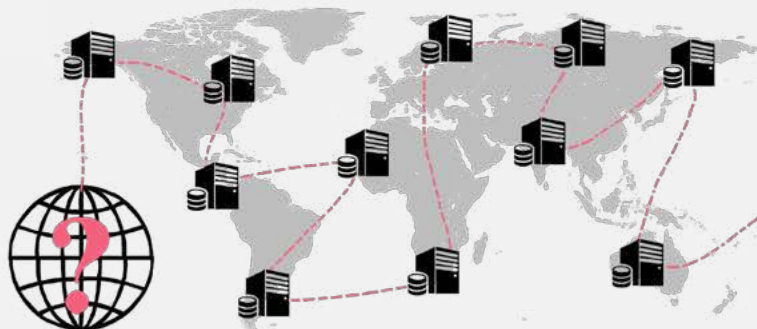
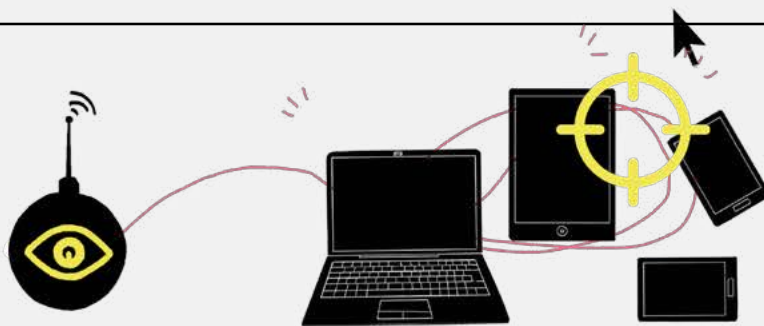
21 Support@hackingteam.it. “Exploit Requests”. E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/640759>; Support@hackingteam.it. “HTML Exploit”. E-mail. 8 de Julio de 2015. Wikileaks <https://wikileaks.org/hackingteam/emails/emailid/532912>; Support@hackingteam.it. “Exploit Docx”. E-mail. 8 de Julio de 2015. Wikileaks <https://wikileaks.org/hackingteam/emails/emailid/529235>

FIGURA 1:

¿CÓMO FUNCIONA REMOTE CONTROL SYSTEM?

Remote Control System puede atacar computadores de escritorio y portátiles, teléfonos móviles y tablets.

Los dispositivos de las víctimas son **inoculados** a través de alguno de los métodos contemplados por RCS: vía USB, a través de la red WiFi, links maliciosos, *exploits* y otros.

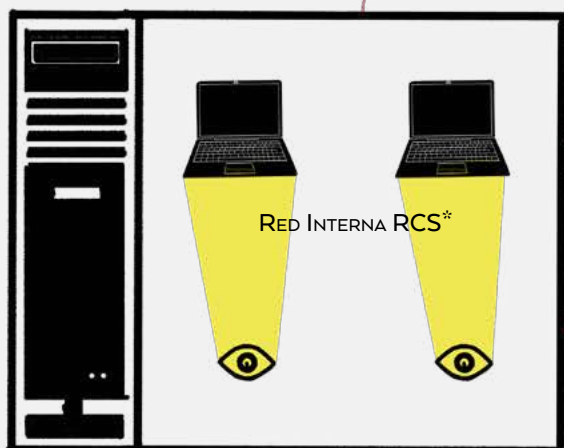


Los dispositivos inoculados envían la información de la víctima a través de internet. Los datos pasan por una serie de *anonymizers*, servidores distribuidos alrededor del mundo que mantienen anónima la comunicación entre los dispositivos infectados y el *collector*.



Toda la información de las víctimas es recibida en el *collector* y, desde ahí, distribuida a la red interna de RCS.

Un *firewall* protege la red interna de RCS del exterior



Una vez en la red interna de RCS, la información de las víctimas puede ser revisada por los operadores, funcionarios gubernamentales capacitados por Hacking Team.



*Para efectos de simplicidad se han omitido componentes de la red interna de RCS.

blico (es decir, que se puede acceder desde internet) llamado *Collector*.

2) *Collector*. Es una especie de enrutador 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.

3) *Software* espía. Para cada dispositivo, teléfono celular o computadora de la persona infectada, se debe instalar un programa distinto. Su función es recopilar y enviar la información de cada dispositivo a la cadena de *Anonymizers*.

4) *Anonymizers*. Servidores distribuidos geográficamente alrededor del globo cuya función es mantener la comunicación entre los *software* espías 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 crea una cadena de servidores que transportan la información recolectada desde las víctimas hasta el *Collector*, creando capas de anonimato que dificultan el rastreo de información hasta los servidores gubernamentales.

¿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”.

Esto funciona de dos formas. Primero, porque los manuales de Hacking Team recomiendan a sus clientes adquirir certificados de Verisign (ahora Symantec), Thawte o GoDaddy, que permiten que el navegador o la aplicación que recibe el *malware* lo haga tomando el *software* como legítimo, de modo que la capacidad invasiva sea más difícil de detectar.²²

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.²³ 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. En ambos se utilizan varias capas y saltos para evitar la revelación de identidades en el emisor y el destino de los datos; en el caso de RCS, dichas capas y saltos son provistos por los *Anonymizers* mencionados previamente.²⁴

22 “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”. Corra Currier, y Morgan Marquis-Boire. “Secret Manuals Show the Spyware Sold to Despots and Cops Worldwide”. The Intercept. 30 de octubre de 2013. Consultado el 8 de noviembre de 2015. <https://theintercept.com/2014/10/30/hacking-team/>

23 Ídem

24 Our research reveals that the RCS collection infrastructure uses a proxy-chaining technique which is roughly

En definitiva, se trata de *software* con gran poder intrusivo, que se introduce en equipos permitiendo su control a distancia, con importantes riesgos sobre la seguridad de los equipos y sobre la privacidad de sus usuarios. Cabe preguntarse si su adquisición y su uso por agentes gubernamentales constituye una interceptación legal sobre esas personas.

analogous to that used by general-purpose anonymity solutions like Tor in that multiple hops are used to anonymize the destination of information. Despite this technique, we are still able to map out many of these chains and their endpoints using a specialized analysis. Bill Marczak, Claudio Guarnieri, Morgan Marqui S - Boire, y John Scott - Railton. "Mapping Hacking Team's 'Untraceable' Spyware". Munk School of Global Affairs, 14, de febrero de 2014, 1-9. Consultado el 8 de noviembre de 2015 <https://citizenlab.org/wp-content/uploads/2015/03/Mapping-Hacking-Team's-Untraceable-Spyware.pdf> (Traducción de la autora)

3. Panorama legal en América Latina

3.1. Interceptación de equipos y derechos humanos

La premisa de este informe es que una tecnología tan invasiva y poco regulada como la 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 están íntimamente relacionados, pues la vigilancia de este tipo crea un efecto silenciador en las expresiones.²⁵

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

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.²⁶

Es importante dejar claro que la tecnología de RCS oscila entre la interceptación de comunicaciones y los allanamientos o pesquisas de lugares físicos por parte de las autoridades. Sin embargo, a diferencia de ambas actividades, el *software* de Hacking Team implica un nivel de interceptación mayor, que no está expresamente regulado y sobre el que tampoco existen mecanismos de control. A falta de esto, no existen reglas de control anterior o posterior que permitan resguardar 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. En esa medida, es violatorio de derechos humanos.

Los Estados deben garantizar que la interceptación, recolección y uso de información personal (...) estén claramente autorizadas por la ley a fin de proteger a la persona contra interferencias arbitrarias o abusivas en sus intereses 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.²⁷

25 Relator Especial de las Naciones Unidas 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". Organización de los Estados Americanos. Consultado el 15 de enero de 2015. <https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=926&IID=2>

26 Ídem

27 Ídem

Conforme a un tradicional principio legal, mientras los ciudadanos pueden 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.²⁸

Esto representa un riesgo particularmente grave 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. Si hoy en día todo es digital, las fotografías, documentos, cartas y mensajes ya no existen de manera física. Es más: el historial de uso de dispositivos electrónicos con acceso a internet es mucho más revelador de nuestra personalidad e intereses que los rastros físicos presentes en un hogar.

En la mayoría de los casos, la interceptación de comunicaciones requiere una orden judicial. Pero como el *software* de RCS puede hacer mucho más, la orden referida a la mera interceptación no es suficiente. Tomando esto en cuenta, la pregunta central se convierte en: ¿es legal este tipo de *software* en América Latina?

En este sentido, los alcances del uso de RCS pueden dividirse para ser analizados a partir de varios marcos legales específicos. Uno de ellos es la interceptación de comunicaciones 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 necesita siempre de una orden judicial como medida de control para poder justificarlo.

El segundo parámetro se refiere a las reglas sobre geolocalización de personas a partir de dispositivos como celulares y computadoras. También vale la pena revisar otros modos de inspección de bienes físicos de una persona investigada, como son las reglas relativas al allanamiento de domicilios e incautación e inspección de objetos, pues en estos últimos suelen establecerse límites específicos que debe contener la orden judicial, no todos los bienes de una persona sospechosa pueden ser inspeccionados. Es decir que, aún en el marco de procesos penales, hay objetos personales de los acusados que siguen siendo protegidos por las leyes, requisitos que cumplir para la procedencia de la medida y el resguardo de los intereses del afectado sobre sus bienes. Si el *software* de Hacking Team por sus capacidades tecnológicas es más invasivo que un allanamiento o inspección física, como mínimo se deberían respetar estándares análogos a los de estos casos.

Ciertos países regulan alguno de estos supuestos. Si está normada la interceptación 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 básicos como los principio de legalidad y seguridad jurídica.

Hay que agregar que las capacidades de RCS son una forma de intervención que podríamos

28 Max Weber. “La Política Como Vocación”. El Político y el Científico. Alianza Editorial; 2. 1919.

calificar como una hipótesis que cabe dentro de la definición de “abuso de dispositivos” del artículo 6 del Convenio de Budapest. Este instrumento establece que se debe sancionar penalmente la producción, venta, obtención, importación, difusión o puesta a disposición de dispositivos -incluyendo programas informáticos- destinados a la comisión de delitos como acceso ilícito a sistemas informáticos, interceptación ilícita de datos o transmisiones no públicas y ataques a la integridad de sistemas.²⁹ Aun cuando la mayoría de los países de la región no han adherido al tratado (se encuentra en vigor en República Dominicana y Panamá), es relevante considerar, para efectos de cualquier implementación futura, que la intrusión al estilo RCS consistiría en una de las conductas que se busca sancionar como ciberdelito.

Si a esto sumamos el uso clandestino y la naturaleza reservada de las actividades de espionaje estatal, se presenta una paradoja adicional, pues si bien estas formas de acción 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.

3.2. Adquisición estatal de *malware* para la vigilancia de comunicaciones

En América Latina, son pocos los países que no tuvieron contacto con Hacking Team: Brasil, Chile, Colombia, Ecuador, Honduras, México y Panamá compraron el programa de la empresa en distintas cantidades y a distintos precios. Adicionalmente, Argentina, Guatemala, Paraguay, Uruguay y Venezuela hicieron negociaciones, aunque no concretaron la compra dentro del período de comunicaciones filtradas a internet.

Dado que Hacking Team es una compañía italiana, todos sus productos están sujetos a las normas sobre restricción de importaciones de países de la Unión Europea. A partir de enero de 2015, la Regulación 429/2008 Para Tecnologías de Doble Uso, restringe la exportación de *software* intrusivo como Remote Control System.³⁰ Estos desarrollos se basan en los pactos hechos con base en el Arreglo de Wassenaar sobre control de exportaciones de Armas Convencionales y bienes y tecnología de Doble Uso,³¹ un régimen intergubernamental utilizado para definir y determinar qué productos deben ser sujetos a licencia para exportarlos y fomentar la seguridad internacional.³²

Debido a estas condiciones de restricción a la venta directa por parte de la empresa italiana, los gobiernos hicieron contacto con Hacking Team a través de empresas intermediarias. La empresa más predominante en la región fue Robotec, originaria de Colombia, presente en este país y con filiales que negociaron dicho *software* en Ecuador y Panamá. En

29 Council of Europe. “Convenio sobre la Ciberdelincuencia”. 23 de septiembre de 2001. Consultado el 4 de marzo de 2016. https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF

30 “Hacking Team Manifest”. Pastebin. 7 de julio de 2015. Consultado el 9 de marzo de 2016. <http://pastebin.com/TKK7BCSK>

31 “The Wassenaar Arrangement On Export Controls for Conventional Arms and Dual-Use Goods and Technologies”. The Wassenaar Arrangement Home Webpage. Consultado el 11 de enero de 2016. <http://www.wassenaar.org/>

32 “Briefing for the Italian Government on Hacking Team”. Privacy International. Abril y mayo de 2015. Consultado el 19 de septiembre de 2015. <https://privacyinternational.atavist.com/hackingteamsurveillanceexports>

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 dedicado a la venta de armas AK-47 que eventualmente terminaron en manos de grupos paramilitares colombianos.³³

Aunque no es el objetivo del presente trabajo, una pregunta subyacente es si dichas empresas –bajo los “Principios Rectores sobre las empresas y los derechos humanos”– tendrían algún tipo de responsabilidad en los casos en que se comprobó que los programas fueron utilizados para espiar a disidentes, periodistas y opositores políticos.³⁴

3.3. Regímenes legales de investigación mediante medidas intrusivas

En 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 cumplimiento de requisitos procesales 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 autorización legal o una orden judicial que autorizara la infección, la prueba debe ser desechada por ser ilegal.

En la región, los límites y modalidades de dicha interceptación 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, 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 renovables.

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

33 Lee Fang, “Former AK-47 Dealer Goes Cyber, Supplied Surveillance Tools to Honduras Government”. The Intercept. 27 de julio de 2015. Consultado en Marzo de 2016. <https://theintercept.com/2015/07/27/ak-47-arms-dealer-goes-cyber-supplied-surveillance-tools-honduras-government/>

34 Principios Rectores sobre las empresas y los derechos humanos: puesta en práctica del marco de las Naciones Unidas para “proteger, respetar y remediar”. Informe del Representante Especial del Secretario General para la cuestión de los derechos humanos y las empresas transnacionales y otras empresas, John Ruggie. Consejo de Derechos Humanos. 17º período de sesiones. Consultado el 10 de octubre de 2015. <http://www.global-business-initiative.org/wp-content/uploads/2012/07/GPs-Spanish.pdf>

En Chile, Honduras, Argentina, Paraguay y Panamá deben además existir sospechas de participación en el delito o relación con el proceso para que la medida sea aceptada. En Guatemala y Paraguay todo lo que no esté relacionado con la causa investigada debe destruirse. Pocos países tienen este estándar.

Una 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 parejas o aquellas que guardan secretos profesionales sobre las personas investigadas. En otros lugares, los resultados y diagnósticos médicos también están exentos. Estos límites son importantes si pensamos en un *software* como el de Hacking Team que, por sus capacidades invasivas, no discrimina entre comunicaciones protegidas que jamás pueden ser secuestradas o analizadas.

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

En Colombia, por ejemplo, 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, entre los organismos que efectivamente compraron licencias de los programas de Hacking Team, la Policía de Investigaciones de Chile y la Policía Federal de Brasil 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 interceptar comunicaciones. En cualquier caso, el estándar de la orden judicial debe ser preservado. Esto, sin perjuicio de la consideración ya reiterada, de que RCS va más allá de una simple interceptación de comunicaciones.

El caso mexicano es particular en este contexto, pues como se explica posteriormente, ocho de las diez autoridades que compraron el *software* no están facultadas para ejercer actividades de vigilancia de comunicaciones, y aún menos para interceptar equipos a distancia, por lo que su uso de RCS es ilegal.

Detectamos también una tendencia particular en países como Colombia, Ecuador y Méxi-

co: a pesar de que existen sólidos marcos legales que protegen derechos humanos y regulan la interceptación 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 de la autoridad pueden ser contrarias a la legislación sin que exista una sanción adecuada.

Por último, llama la atención que todos los países que compraron RCS cuentan con sanciones penales en caso que se invadan o intervengan los sistemas informáticos o comunicaciones privadas de una persona fuera de la legalidad de una investigación. Así, Brasil criminaliza la invasión de dispositivos informáticos con el fin de obtener datos; Chile castiga al funcionario público que busque usar o conocer la información contenida en un sistema informático o que lo haga para amenazar o perjudicar a una persona específica; México y Panamá sancionan la interceptación de comunicaciones privadas sin orden judicial y Honduras, por otro lado, sanciona únicamente a funcionarios públicos o empresas que divulguen la información interceptada. Además, son aplicables las reglas sobre ciberdelitos, allí donde tales reglas existen.

Colombia y Ecuador tienen una regulación muy amplia en la materia, pues no solo sanciona a quien sustraiga, intercepte o controle una comunicación privada, sino también a quien, sin permiso, ofrezca, venda o compre *software* malicioso o enlaces y ventanas para realizar estos fines. Con este marco normativo, ¿deberían estos países abrir un proceso contra Robotec o Hacking Team? Salvo en Panamá, en ningún otro país se han abierto investigaciones, a pesar de que la legislación lo contempla.

4. Clientes de Hacking Team en América Latina

4.1 Brasil

En julio de 2013, poco tiempo después de las revelaciones de Edward Snowden, el periódico brasileño O Globo reveló que la National Security Agency de Estados Unidos había espiado dos mil trescientos millones de llamadas y mensajes de ciudadanos brasileños a través del programa Fairview.³⁵ El Gobierno y la entonces presidenta Dilma Rousseff catalogaron este tipo de vigilancia como “extremadamente grave”, por violar la Constitución de Brasil y afectar el derecho a la inviolabilidad de las comunicaciones.³⁶ Exigieron una respuesta a Estados Unidos, cosa que pocos otros países se atrevieron a hacer frente a casos similares.

Sin embargo, y a pesar de estas declaraciones internacionales anti-vigilancia, la Policía Federal Brasileña compró el *software* de Hacking Team, mientras que otras entidades estatales se reunieron con la empresa.

La primera persona que llevó la tecnología de Hacking Team a Brasil en 2011 fue Gualter Tavares Neto, ex-secretario adjunto de Transporte del Distrito Federal, mediante su empresa Defence Tech.³⁷ En los correos con el personal de Hacking Team, Tavares preguntaba si DaVinci y Galileo eran mejores que servicios similares de Elbit Systems, Finfisher y Gamma Group.

Cuatro años después de ese primer contacto, en mayo de 2015 la Policía Federal firmó un contrato con el intermediario YasniTech (la empresa que trianguló la operación) para adquirir el *software* de Hacking Team y utilizarlo en el marco de un proyecto piloto que duraría tres meses.³⁸ Pagaron un precio total de 75 mil reales a YasniTech.³⁹ A su vez, YasniTech pagó a Hacking Team una suma de 25 mil euros por la licencia del programa.⁴⁰ Se esperaba que para el tercer semestre del 2015 se cerrara la venta de 1.750.000 euros más.⁴¹

35 Glen Greenwald. “EUA Espionaram Milhões De E-mails E Ligações De Brasileiros”. O Globo. 12 de julio de 2013. Consultado el 9 de marzo de 2016. <http://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934>

36 Ídem

37 Natalia Viana. “Hackeando O Brasil”. Pública. 27 de julio de 2015. Consultado el 8 de febrero de 2016. <http://apublica.org/2015/07/hackeando-o-brasil/>

38 M.luppi@hackingteam.com. “Defense Tech / HT - Business in Brazil - Your best attention” E-mail. 8 de Julio de 2015. <https://www.wikileaks.org/hackingteam/emails/emailid/7226>

39 Natalia Viana. “Em Parceria Com PF, Empresa De Software Espião Estaria Hackeando O Brasil - Notícias - Tecnologia”. UOL Notícias. 28 de julio de 2015. Consultado el 9 de marzo de 2016. <http://tecnologia.uol.com.br/noticias/redacao/2015/07/28/em-parceria-com-pf-empresa-de-software-espiao-estaria-hackeando-o-brasil.htm>

40 Luca.gabrielli@yasnitech.com.br. “Pagamento e programmazione”. E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/7014>

41 Redação Linha Defensiva. “Linha Defensiva”. PF Estava Para Fechar Contrato Milionário De Espionagem. 27 de julio de 2015. Consultado el 9 de febrero de 2016. <http://www.linhadefensiva.org/2015/07/pf-estava-para->

La propuesta era operar tres meses con diez agentes; el precio incluía el *software* necesario, entrenamiento y soporte para este periodo. Por otro lado, el hardware, la renta de la red de anonimato y la conexión a internet serían responsabilidad de la Policía Federal.⁴² El proyecto piloto sería utilizado por el Departamento de Crímenes Hacendarios y, una vez que se comprobara su eficacia, se implementaría por los departamentos de la Directoría de Investigación y Combate al Crimen Organizado (DICOR) y la Directoría de Inteligencia Policial (DIP), ambos de la Policía Federal.⁴³

Después de las filtraciones de junio de 2015, en una entrevista con el periódico *Pública*, el Comandante del Centro de Instrucción de Guerra Electrónica (CIGE) –una entidad que se encarga de capacitar al Ejército en cuestiones de seguridad digital⁴⁴– reconoció haber tenido contacto con la empresa, pero negó cualquier tipo de compra.⁴⁵ No obstante, se comprobó que Hacking Team efectivamente sostuvo diversas reuniones con este organismo y con el Comando de Aeronáutica, el Departamento de Inteligencia de la Policía Civil del Distrito Federal y de Río de Janeiro, el Departamento de Policía Federal en Brasilia, la Procuraduría General de la República y la Policía Militar del Estado de São Paulo. Al parecer ninguna dependencia concretó compras.

Llama la atención que en uno de los correos intercambiados, Luca Gabrielli de la empresa 9isp (que asumió las negociaciones después de YasniTech) especificó que no existía “ninguna legislación específica o una doctrina legal clara para el uso de un producto como el de Hacking Team”.⁴⁶ Sin embargo, en otro correo se hace referencia a una orden judicial expedida en el primer semestre de 2015 que daba a la Policía Federal el amparo legal para el uso del *software* adquirido para usarse en 17 teléfonos durante 15 días a partir de su instalación.⁴⁷ La lógica subyacente es que, siendo cierto que en Brasil la tecnología de RCS no está expresamente regulada, algunas de sus capacidades podrían justificarse en el marco de la norma de interceptación de comunicaciones y geolocalización.

Hay que mencionar que según el artículo 158 de la Ley 13.097 de enero del 2015, la policía y el Gobierno no necesitan de un proceso de licitación cuando se trata de comprar equipos

fechar-contrato-milionario-de-espionagem/

42 Luca.gabrielli@yasnitech.com.br. “Proposta para piloto HT”. E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/439854>

43 Luca.gabrielli@yasnitech.com.br. “Progetto Polizia Federal”. E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/6963>

44 “Portal De Educação Do Exército Brasileiro”. Ensino. 2015. Consultado el 9 de marzo de 2016. <http://www.ensino.eb.br/exibeDetalhesCurso.do?curso=418>

45 Ibidem. *Pública*.

46 Luca.gabrielli@9isp.com.br. “Intrusão e controle para smartphone”. E-mail. 8 de Julio de 2015. Wikileaks. <https://www.wikileaks.org/hackingteam/emails/emailid/440433>

47 D.vincenzetti@hackingteam.com. “Brenda Operation”. E-mail. 8 de Julio de 2015. Wikileaks. <https://www.wikileaks.org/hackingteam/emails/emailid/921908>

necesarios para investigaciones policiales. Esta regulación básicamente les da carta blanca en la adquisición de este tipo de *software*.

Intercepción de comunicaciones durante un proceso penal

El artículo 5 fracción XII de la Constitución de Brasil establece el derecho a la inviolabilidad y secreto de las comunicaciones. Las comunicaciones telefónicas solo pueden ser intervenidas por orden judicial y para fines de investigación criminal o de instrucción en el proceso penal. Las leyes N° 9.472/97 (artículos 3°, V y IX) y la N° 12.965/14 (artículo 7°) garantizan también el derecho al sigilo de las comunicaciones y a la privacidad en el uso de la telefonía e internet.⁴⁸

En sí, las reglas para interceptar están principalmente en la Ley No 9.296 de 1996, en la que se establece que toda interceptación de comunicaciones en sistemas informáticos o telemáticos (incluyendo internet) debe ser autorizada por un juez. Las autoridades policiales o representantes del Ministerio Público son quienes pueden pedir las, pero no se puede admitir si a) no hay indicios razonables de la autoría o participación en delitos penales graves o b) si la prueba se puede obtener por otros medios. El plazo inicial es de 15 días, que pueden ser renovables.⁴⁹

Por otro lado, según el artículo 157 del Código de Proceso Penal, si durante la interceptación se obtiene información adicional sin contar con orden judicial, esta no podría ser presentada como prueba en un proceso porque sería inválida. Es decir que si se instala el *software* de Hacking Team en una computadora o celular sin orden judicial, aunque se encuentren pruebas que sirvan para acreditar la culpabilidad de un delito, las mismas no deben ser admitidas por contravenir el derecho humano a la inviolabilidad de las comunicaciones.

Pero el Código de Proceso Penal, en su artículo 6 fracción III contiene una facultad tan amplia que puede abrir la puerta para la justificación legal de un *software* como el de Remote Control System. Se establece que la autoridad policial después de tener conocimiento sobre una infracción penal debe obtener “todas las pruebas” que puedan servir para esclarecer los hechos.⁵⁰ En esta misma línea, la Ley 12.830 prevé que, durante una investigación criminal, el delegado de la policía puede requerir peritajes, informaciones, documentos o datos que ayuden a aclarar los hechos. Sin embargo, en ambos casos se tendría que seguir la regla general del artículo 130, que exige contar con una orden judicial en los casos que la producción de pruebas restrinja derechos protegidos por la Constitución.

Una ventaja de la legislación brasileña, que no necesariamente se reproduce en la región,

48 Dennys Antonialli, y Jacqueline De Souza Abreu. “Vigilância Das Comunicações Pelo Estado Brasileiro E a Proteção a Direitos Fundamentais”. Electronic Frontier Foundation e Internet Lab, 2015, 11-12. Consultado el 9 de febrero de 2016. http://www.internetlab.org.br/wp-content/uploads/2015/11/VigilanciaEstado_Diagram_vprova.pdf.

49 Ibidem, 24-25.

50 Ídem

es que el Marco Civil de Internet establece en su artículo 7 que los usuarios de internet que vean afectado su derecho a la inviolabilidad de las comunicaciones y vida privada en la red tienen derecho a ser indemnizados por daño material o moral. Esto se traduce en que si cualquier persona es espiada fuera de procesos judiciales o en el marco de actividades de inteligencia sin orden judicial, puede pedir indemnización.

Geolocalización

Con lo que respecta a la regulación sobre localización geográfica a partir de aparatos de tecnología, Internet Lab precisa que esta misma no se encuentra tipificada, pero puede permitirse en el marco de una orden judicial.⁵¹

Interceptación de equipos y comunicaciones por organismos de inteligencia

Fuera de procesos judiciales, la interceptación de comunicaciones también se puede dar en el marco de actividades de inteligencia. Según la Ley 833/99 corresponde al órgano central del Sistema Brasileiro de Inteligência, la Agencia Nacional de Inteligencia, “planear, ejecutar, supervisar y controlar” estas actividades.⁵² Por el Decreto 4.376, también forman parte del Sistema de Inteligencia la Casa Civil, el Gabinete de Segurança Institucional de la Presidencia y los diversos Ministerios y órganos relacionados (entre ellos la Policía Federal, el Ministerio de Justicia y el Ministerio de Hacienda).⁵³

La Agencia Nacional de Inteligencia no tiene facultades propiamente dichas para obtener información, pero sí puede obtener datos mediante los órganos que componen el Sistema Nacional de Inteligencia. Según el Decreto 4.376, no existen impedimentos para el monitoreo de comunicaciones privadas, pero al no haber facultades expresas, tampoco puede deducirse.⁵⁴

Analizando las facultades de la Policía Federal que adquirió el *software* de Hacking Team, concluimos que sí puede monitorear comunicaciones y realizar ciertas actividades de vigilancia e inteligencia, pero que esas capacidades no necesariamente se extienden a un control total sobre el equipo intervenido. Específicamente, la parte de la Policía llamada Diretoria de Inteligência es la facultada para dirigir, planear, coordinar, controlar, avalar y orientar estas actividades según el artículo 15 del Reglamento Interno de este organismo. De cualquier forma, según el análisis de los correos filtrados por Pública, cuando la Policía Federal adquirió el *software* de espionaje de Hacking Team, lo hizo con la debida autorización judicial.⁵⁵

Sanciones

A los funcionarios públicos que hayan utilizado el *software* de Hacking Team sin una debida orden judicial se les sanciona con dos a cuatro años de prisión y multa. La Ley 9.296

51 Ibidem, 11.

52 Ibidem, 11-12.

53 Idem

54 Idem

55 Natalia Viana. “Hackeando O Brasil”. Pública. 27 de julio de 2015. Consultado el 8 de febrero de 2016. <http://apublica.org/2015/07/hackeando-o-brasil/>

castiga así a quienes intercepten comunicaciones telefónicas, informáticas o telemáticas, o quiebren el secreto de justicia sin autorización judicial o con objetivos distintos a los de investigación judicial en procesos penales.

De la misma forma, el artículo 2° de la Ley 12.737 castiga con tres meses a un año de prisión a quien invada un dispositivo informático ajeno, mediante la “instalación de vulnerabilidades” con el fin de obtener, adulterar o destruir información sin autorización del titular. La misma pena se le aplica a “quien produzca, ofrezca, distribuya, venda o difunda un programa de computación con la intención de permitir esta conducta”. En este caso, si la empresa Hacking Team vende precisamente este tipo de programas, habría que preguntarse si procedería una sanción penal en su contra.

Por último, el artículo 156-A del Código Penal criminaliza la invasión de dispositivos informáticos con el fin de obtener datos. La pena es de tres meses a un año de detención y multa.

4.2. Chile

El primer contacto de Hacking Team con Chile fue a través de Jorge Lorca, director de la empresa Mipoltec, en agosto de 2013.⁵⁶ Lorca le escribió a Alex Velasco, gerente regional de Hacking Team, para agendar cuatro reuniones con la Policía de Investigaciones de Chile, Carabineros de Chile, el Ejército y la Armada. La relación con la Policía de Investigaciones se formalizó en noviembre de 2014, específicamente con el Departamento de Monitoreo Telefónico (Demtel).⁵⁷ El monto total gastado fue de 2,89 millones de euros.⁵⁸

Originalmente, este organismo rehusó confirmar la compra del *software* de espionaje, pero el día 6 de julio de 2015 emitió un comunicado oficial reconociendo su adquisición.⁵⁹ Se mencionaba que la vigilancia se hacía con fines estrictamente legales y bajo orden judicial, aunque esto no ha sido comprobado.⁶⁰

Según los correos de Hacking Team,⁶¹ el Departamento de Investigación Electrónica de la Policía de Investigaciones es el único cliente chileno de la empresa, aunque existirían más organismos interesados, incluyendo al Ejército y otros departamentos de la misma Policía

56 Barbara Partarrieu, y Matías Jara. “Los Correos que Alertaron Sobre la Compra del Poderoso Programa Espía de la PDI”. CIPER Centro de Investigación Periodística. 10 de julio de 2015. Consultado el 9 de marzo de 2016. <http://ciperchile.cl/2015/07/10/los-correos-que-alertaron-sobre-la-compra-del-poderoso-programa-espia-de-la-pdi/>

57 Ibid.

58 Ibid.

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

60 Ídem

61 “Hacking Team, Chile y Ecuador”. People Tor Project. 11 de julio de 2015. Consultado el 16 de septiembre de 2015. https://people.torproject.org/~ilv/ht_chile_ecuador.html

de Investigaciones.⁶² Este organismo quería *software* espía principalmente para sistemas Android, utilizando URL maliciosas que redirigen a sitios de venta populares en Chile (como Dafiti, Falabella o Ripley) o de cupones de descuento (como Groupon).⁶³

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

El artículo 9 del Código Procesal Penal establece que, 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.

Intercepción de comunicaciones privadas en procesos penales

De acuerdo con los artículos 79 y 83 del Código Procesal Penal, la Policía de Investigaciones de Chile no puede interceptar comunicaciones privadas sin que primero el Ministerio Público lo ordene primero; a su vez, esta orden debe estar precedida de una autorización judicial previa que permita su ejecución.

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. El Ministerio Público es el que está facultado para pedir al juez que ordene la interceptación y grabación de las comunicaciones telefónicas y cualquier “otras formas de telecomunicación”. El plazo no puede exceder de 60 días prorrogables. Como excepción, no se pueden interceptar las comunicaciones entre el imputado y su abogado, a menos que el juez de garantía lo ordene.

Debemos recordar que la naturaleza del *software* de Hacking Team es tan invasiva que tiene acceso a todo, incluyendo a las comunicaciones especialmente protegidas, sin que existan los mecanismos adecuados para controlarlo. 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”. Esta redacción parece abrir 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. De igual manera, 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.

Incautación de objetos

Podría establecerse una relación análoga entre la infección del RCS y la incautación de una

62 Ibidem, CIPER Centro de Investigación Periodística.

63 Ibidem, People Tor Project.

computadora o un teléfono celular. Si bien no es una “incautación física” ni una sustracción de objetos, el efecto es similar, pues permite analizar un objeto en búsqueda de 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”.

Interceptación de comunicaciones por aparatos de inteligencia

En 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 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 interceptación de las comunicaciones telefónicas, informáticas, radiales y de la correspondencia en cualquiera de sus formas;
- b) La interceptación de sistemas y redes informáticos;
- c) La escucha y grabación electrónica incluyendo la audiovisual, y
- d) La interceptación de cualesquiera otros sistemas tecnológicos destinados a la transmisión, almacenamiento o procesamiento de comunicaciones o información.

Si interpretamos de forma amplia las capacidades de “interceptación”, el uso del *software* de Hacking Team estaría respaldado por este artículo, particularmente en sus incisos 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 concierne a 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 también se

extiende a los funcionarios estatales (como los tribunales o miembros del Congreso) encargados del control de la actividad de inteligencia que soliciten 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).

No existe el deber de notificar a las personas sujetas a una investigación no formalizada en ninguno de los dos sistemas. 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 interceptación 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 interceptación de comunicaciones o equipos en los casos en que un juez lo permita, a petición del propio Ministerio Público o los organismos de inteligencia en el marco de la ley respectiva. 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 Policía de Investigaciones esté cubierto por el ordenamiento jurídico chileno. No se pueden dejar de lado los derechos humanos, plasmados en la Constitución y afectados por el uso de este tipo de *software*, ni las expectativas de seguridad y privacidad existentes sobre el sistema informático que se utilice. El uso de 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. No basta con interpretar ampliamente facultades legales, el uso de *software* que vulnera la integridad de sistemas y recoge cantidades ingentes de información no es parte de las autorizaciones legales.

Sanciones

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 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 utilice 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.

4.3. Colombia

Desde principios de la década de los sesenta, Colombia se envolvió en una lucha contra el narcotráfico que marcó a más 46 millones de personas y dejó cerca de 20.000 víctimas, gastando más de 10.000 millones de dólares en las últimas tres décadas en su erradicación.⁶⁴

La vigilancia de las comunicaciones es parte del conflicto.⁶⁵ Según el informe “Un estado en la sombra: vigilancia y orden público en Colombia”, de Privacy International, desde 2002 se sabe que alrededor de 2.000 líneas telefónicas -entre ellas las de grupos que representaban a familias de las personas desaparecidas- han estado intervenidas.⁶⁶ En 2007 se destituyó a 11 policías por escuchar ilegalmente a políticos de la oposición, periodistas, abogados y activistas. En 2009 se reveló que el Departamento Administrativo de Seguridad (DAS) había vigilado y hostigado a más de 600 figuras públicas. Cinco años más tarde se supo que la unidad del Ejército con el nombre clave “Andrómeda” había estado espiando durante más de un año al equipo negociador del Gobierno en las conversaciones de paz entabladas con las FARC.

Este informe concluyen que los organismos están creando sus propios sistemas de vigilancia en la sombra, sin escrutinio suficiente ni base legal. Según Privacy International:

El gobierno colombiano ha reformado su legislación sobre vigilancia, cuestionado sus capacidades técnicas, e incluso ha disuelto uno de sus organismos de seguridad tras conocerse el uso indebido de los sistemas de vigilancia (...) las recientes reformas se han visto menoscabadas por el despliegue subrepticio de sistemas de vigilancia automatizada y masiva de las comunicaciones, llevado a cabo por varios organismos del Estado fuera del ámbito de lo proscrito por la deficiente legislación colombiana sobre actividades de inteligencia.⁶⁷

En este contexto, el contacto entre las autoridades colombianas y Hacking Team viene por

64 Jineth Bedoya Lima. “Guerra Contra el Narcotráfico: 20 Años de Dolor, Muerte y Corrupción”. El Tiempo. 24 de noviembre de 2013. Consultado el 9 de enero de 2016. <http://www.eltiempo.com/archivo/documento/CMS-13218657>.

65 Privacy International. “Un Estado En La Sombra: Vigilancia Y Orden Público En Colombia”. Informe Especial, agosto de 2015, 7. Consultado el 4 de enero de 2016. https://www.privacyinternational.org/sites/default/files/ShadowState_Espanol.pdf.

66 Ídem

67 Ídem

lo menos desde 2008, cuando representantes del entonces Departamento Administrativo de Seguridad (DAS) se reunieron con el personal de la empresa.⁶⁸

De acuerdo con Fundación Karisma, los documentos filtrados plantean que, en Colombia, Galileo ha sido objeto de dos procesos contractuales. El primero fue con Robotec, la empresa predilecta de Hacking Team en América Latina. Se firmó en 2013 y está vigente hasta 2016. El segundo se refiere a un proceso de contratación que estaba casi cerrado con la empresa israelí NICE al momento de la filtración; de haberse concretado estaba extendido hasta 2018.⁶⁹

Dentro de la Policía Nacional de Inteligencia, la Dirección de Inteligencia de la Policía (Dipol) compró el *software* de Hacking Team por 335 mil euros, con Robotec como socio. Posteriormente compró otra licencia de 850 mil euros a la empresa Nice y además pagaron 35 mil euros por concepto de mantenimiento anual.⁷⁰

En entrevista con el periódico El Tiempo, la Policía señaló que “no ha sostenido vínculo comercial con la firma Hacking Team”, sino con Robotec Colombia S.A.⁷¹ de la cual, en diciembre de 2013 adquirió una herramienta tecnológica para “potencializar la capacidad de detección de amenazas del terrorismo y criminalidad organizada en el ciberespacio colombiano”.⁷² Además hicieron énfasis en que dicho instrumento fue adquirido de manera legal y que “en ningún caso compromete la seguridad ni la privacidad de los colombianos”.⁷³

En general, el panorama de espionaje en Colombia llama particularmente la atención en un doble sentido. Primero, porque los dos contratos se realizaron con fondos destinados a fortalecer la Plataforma Única de Monitoreo y Análisis (PUMA): una plataforma tecnológica adscrita a la Dirección de Investigación Criminal e Interpol de la Policía (DIJIN) que tiene como fin registrar o verificar información sobre personas vinculadas con investigaciones judiciales y coordina tareas de policía, fiscalía e incluso empresas de telefonía. Se menciona por primera vez en una resolución de 2007 y tiene como fin reemplazar la antigua plataforma de interceptación de comunicaciones Esperanza,⁷⁴ el sistema de interceptación de las

68 Daniel Salgar Antolínez. “Un Mundo de Chuzadas”. El Espectador. 22 de julio de 2015. Consultado el 28 de febrero de 2016. <http://www.elespectador.com/noticias/elmundo/un-mundo-de-chuzadas-articulo-574325>

69 Fundación Karisma. “Sobre Hacking Team En Colombia”. 24 de julio de 2015. Consultado el 6 de enero de 2016. <https://karisma.org.co/sobre-hacking-team-en-colombia/>

70 Pilar Sáenz. “En 2015 Colombia Compró 850 Mil Euros en Software de Hacking Team”. Contagio Radio. July 13, 2015. Accessed March 09, 2016. <http://www.contagioradio.com/en-2015-colombia-compro-850-mil-euros-en-software-de-hacking-team-articulo-11146/>

71 Diana Carolina Durán Nuñez. “El Software Espía de la Policía”. El Espectador. 11 de julio de 2015. Consultado el 9 de marzo de 2016. <http://www.elespectador.com/noticias/investigacion/el-software-espia-de-policia-articulo-571980>

72 Justicia. “Policía Indicó No Tener Vínculos Comerciales con Firma Hacking Team”. El Tiempo. 8 de julio de 2015. Consultado el 9 de marzo de 2016. <http://www.eltiempo.com/politica/justicia/policia-indico-no-tener-vinculos-comerciales-con-firma-hacking-team/16063640>

73 Ídem

74 Pilar Sáenz, y Carolina Botero. “En Colombia, El PUMA No Es Como Lo Pintan”. Digital Rights LAC. Agosto

comunicaciones más notorio de Colombia, que recibe apoyo de la Administración para el Control de Drogas (DEA) de Estados Unidos.⁷⁵

En segundo lugar, porque el periodista Ryan Gallagher divulgó por Twitter un correo electrónico que apunta a una reunión de los miembros de Hacking Team con Michael Casey de la DEA y el Gobierno colombiano.⁷⁶ Aquí se dice que Casey “necesitaría soporte técnico porque compraron otra herramienta de interceptación (que recibe todo el tráfico de todos los ISP de Colombia) y lo instalarán en la habitación en la que, actualmente, tienen las herramientas de control remoto de RCS”.

Según el reporte de Fundación Karisma titulado “Cuando el Estado Hackea”,⁷⁷ se sospecha del uso de herramientas de este tipo contra de la periodista Vicky Dávila, quien denunció la interceptación de sus comunicaciones privadas, las de su familia y de su equipo de trabajo. La motivación parece venir del hecho que estos periodistas tienen información filtrada de una red de prostitución masculina al interior de la propia Policía.⁷⁸

Frente a este panorama de espionaje, ¿es legal el uso de *software* de espionaje de Hacking Team en Colombia? La interceptación de comunicaciones es legal si se realiza con orden judicial, aunque existen casos excepcionales en que la Fiscalía puede hacerla y validar posteriormente su uso con un juez.⁷⁹ Por otro lado, dentro del marco de un proceso judicial se puede ordenar la recuperación de información dejada al navegar por internet u otros medios tecnológicos. Sin embargo, el resto de funciones que RCS puede llevar a cabo no están propiamente reguladas y esto en sí es un problema de legalidad.

Interceptación de comunicaciones privadas en procesos penales

La regla general es que cualquier actividad de la Policía Judicial que afecte derechos humanos solo puede realizarse con autorización previa del juez, a petición del fiscal correspon-

2014. Consultado el 15 de febrero de 2016. <http://www.digitalrightslac.net/es/en-colombia-el-puma-no-es-como-lo-pintan/>

75 “Desde el punto de vista de su funcionamiento, Esperanza es un sistema de interceptación selectiva, que se basa en solicitudes activas de usuarios humanos, los administradores de la Fiscalía, para “encargar” a los proveedores de servicios de Colombia enviar los registros de datos y audio de llamadas de telefonía ja y móvil, solicitados específicamente. Esta actividad está aprobada expresamente por la Constitución y el Código de Procedimiento Penal de Colombia”. Ibidem Privacy International, 14.

76 Félix Palazuelos. “Hacking Team: Todo el Internet de Colombia Interceptado”. Hipertextual. 7 de julio de 2015. Consultado el 23 de septiembre de 2016. <http://hipertextual.com/2015/07/colombia-hacking-team>

77 Juan Diego Castañeda. “Cuando el Estado Hackea: Análisis de la Legitimidad del Uso de Herramientas de Hacking en Colombia”. Fundación Karisma. 10 de diciembre de 2015. Consultado el 15 de enero de 2015. <https://karisma.org.co/wp-content/uploads/2015/12/CUANDO-EL-ESTADO-HACKEA-D.pdf>

78 Daniel Coronell. “Los Caballeros de la Noche”. Semana. 5 de diciembre de 2015. Consultado el 10 de marzo de 2016. <http://www.semana.com//opinion/articulo/daniel-coronell-el-caso-del-general-palmino-la-banda-de-prostitucion-en-la-policia/452337-3>

79 Ibidem, Privacy International. Página 14.

diente, según el artículo 246 del Código de Procedimiento Penal.⁸⁰

Por otro lado, la Constitución colombiana reconoce en su artículo 15 que “la correspondencia y demás formas de comunicación privada son inviolables” y que las mismas solo pueden ser interceptadas o registradas mediante orden judicial. La Corte Constitucional en la Sentencia T-916/2008 reconoció el correo electrónico como un medio de comunicación privado. Por otro lado, el artículo 29 de la Constitución establece que “es nula, de pleno derecho, la prueba obtenida con violación del debido proceso”.

El Código de Procedimiento Penal de Colombia permite la interceptación de comunicaciones en su artículo 235, con una vigencia máxima de tres meses. El artículo 236 establece que si el fiscal tiene motivos razonablemente fundados, puede ordenar la recuperación de información dejada al “navegar por internet u otros medios tecnológicos”. Se justificaría entonces la obtención de información sobre las páginas y sitios de internet visitados por la víctima, otras de las capacidades del programa Galileo.

Incautación de información y objetos

Fuera de la interceptación de comunicaciones, el monitoreo de páginas de internet, chats, mensajes o fotografías almacenadas en el disco duro podrían estar justificadas de acuerdo con el artículo 236 del Código de Procedimiento Penal, siempre y cuando se acredite que el procesado manipuló datos a través de las redes de telecomunicaciones. Es decir, solo se acota a este supuesto legal. En ese caso el juez puede ordenar a Policía Judicial la “retención, aprehensión o recuperación de dicha información, equipos terminales, dispositivos o servidores que pueda haber utilizado cualquier medio de almacenamiento físico o virtual, análogo o digital, para que expertos en informática forense descubran, recojan, analicen y custodien la información que recuperen”.

Interceptación de comunicaciones por organismos de inteligencia

En Colombia, los organismos de inteligencia están autorizados para ejercer actividades de vigilancia, entre las que podría incluirse la interceptación de comunicaciones. La Ley 1621 define las actividades de inteligencia y contrainteligencia como “aquella que desarrollan los organismos especializados del Estado (...) utilizando medios humanos o técnicos para la recolección, procesamiento, análisis y difusión de información, con el objetivo de proteger los derechos humanos, prevenir y combatir amenazas internas o externas contra la vigencia del régimen democrático, el régimen constitucional y legal, la seguridad y la defensa nacional” (artículo 2).

El supuesto legal es demasiado amplio, pues bajo la sombra de un objetivo legítimo puede justificar prácticamente cualquier cosa en términos de espionaje, inclusive si no existe una base razonable de sospecha contra un individuo.

La interceptación de conversaciones privadas telefónicas móviles o fijas, así como de las

⁸⁰ El artículo 161 del Código de Procedimientos Penales define las órdenes judiciales, si son otra cosa que sentencias o autos dentro del proceso, y “se limitan a disponer cualquier otro trámite de los que la ley establece para dar curso a la actuación o evitar el entorpecimiento de la misma”. Son verbales, de cumplimiento inmediato y se debe dejar un registro de la misma.

comunicaciones privadas de datos, deberán someterse a los requisitos establecidos en el artículo 15 de la Constitución y el Código de Procedimiento Penal y solo podrán llevarse a cabo en el marco de procedimientos judiciales.

Por otro lado, el artículo 17 establece que las actividades de inteligencia y contrainteligencia comprenden actividades de monitoreo del espectro electromagnético que, si no sirve para el cumplimiento de los fines establecidos en la ley, deberá ser destruida y no podrá ser almacenada en las bases de datos de inteligencia y contrainteligencia. Dichos fines son: a) asegurar la consecución de los fines esenciales del Estado, la vigencia del régimen democrático, la integridad territorial, la soberanía y la seguridad b) proteger las instituciones democráticas y los derechos frente a amenazas como el terrorismo, el crimen organizado, el narcotráfico, el secuestro, el tráfico de armas, municiones, explosivos, etc. c) proteger los recursos naturales y los intereses económicos de la Nación.

También se establece que las actividades de inteligencia y contrainteligencia no pueden recolectarse en base a criterios de género, raza, origen nacional o familiar, lengua, religión, opinión política o filosófica, pertenencia a una organización sindical, social o de derechos humanos, o para promover los intereses de cualquier partido o movimiento político o afectar los derechos y garantías de los partidos políticos de oposición.

Adicionalmente, el Decreto 857 de 2014 lista otros organismos e instituciones que también pueden llevar a cabo actividades de inteligencia y contrainteligencia.⁸¹

81 1. En las Fuerzas Militares: a) En el Comando General de las Fuerzas Militares:

1. La Jefatura de Inteligencia y Contrainteligencia Militar Conjunta, sus Direcciones, Divisiones y/o equivalentes y demás unidades o dependencias de inteligencia y contrainteligencia subordinadas a ella; 2. Las unidades o dependencias de inteligencia y contrainteligencia en cada uno de los Comandos Conjuntos o Comandos de Fuerza de Tarea Conjunta; 3. Las unidades o dependencias especiales creadas por el Comandante General de las Fuerzas Militares, mediante acto administrativo, para realizar actividades de Inteligencia y Contrainteligencia, previo concepto de la Jefatura de Inteligencia y Contrainteligencia Militar Conjunta, de acuerdo con su misión, competencias y funciones.
 - b) En el Ejército Nacional: 1. La Jefatura de Inteligencia y Contrainteligencia del Ejército Nacional, las dependencias y unidades de inteligencia y contrainteligencia subordinadas a ella; 2. Las dependencias de inteligencia y contrainteligencia en cada División, Brigada, Batallón y unidades que por su naturaleza y misión desarrollen estas actividades en sus diferentes niveles; 3. Las unidades especiales creadas por el Comandante del Ejército, mediante acto administrativo, para realizar actividades de Inteligencia y Contrainteligencia, previo concepto de la Jefatura de Inteligencia y Contrainteligencia Militar, de acuerdo con su misión, competencias y funciones.
 - c) En la Armada Nacional: 1. La Jefatura de Inteligencia Naval, las dependencias y unidades de inteligencia y contrainteligencia subordinadas a ella; 2. Las dependencias de inteligencia y contrainteligencia en cada una de las unidades de la Armada Nacional, que por su naturaleza, misión y organización desarrollen estas actividades en sus diferentes niveles; 3. Las unidades especiales creadas por el Comandante de la Armada Nacional, mediante acto administrativo, para realizar actividades de Inteligencia y Contrainteligencia, previo concepto de la Jefatura de Inteligencia Naval, de acuerdo con su misión, competencias y funciones.
 - d) En la Fuerza Aérea Colombiana: 1. La Jefatura de Inteligencia Aérea, las dependencias y unidades de inteligencia y contrainteligencia subordinadas a ella; 2. Las dependencias de inteligencia y contrainteligencia en cada una de las unidades de la Fuerza Aérea Colombiana, a nivel estratégico, operacional y táctico, que por su naturaleza y misión desarrollen estas actividades en sus diferentes niveles; 3. Las unidades especiales autorizadas por el Comandante de la Fuerza Aérea Colombiana, mediante acto administrativo, para realizar actividades de Inteligencia y Contrainteligencia, previo concepto de la Jefatura de Inteligencia Aérea, de acuerdo con su misión, competencias y funciones.
2. En la Policía Nacional: a) La Dirección de Inteligencia

El artículo 3 establece que los facultados para realizar estas actividades son las Fuerzas Militares, la Policía Nacional y la Unidad de Información y Análisis Financiero; mismos que deben sujetarse siempre a los principios de idoneidad, necesidad y proporcionalidad (artículo 5). En este caso, como ya mencionamos, la Policía Nacional compró el programa de Hacking Team, estando facultada para interceptar comunicaciones según el artículo 17 de la Ley 1621. Sin embargo, las facultades para interceptar comunicaciones no son lo mismo que las facultades para interceptar equipos, pues esta es una medida más invasiva, que no se desprende del artículo mencionado.

Sanciones

Si algún funcionario público llegara a utilizar el *software* de espionaje de Hacking Team sin tener facultades explícitas para ejercer actividades de vigilancia o sin contar con una orden judicial en el marco de un proceso penal, se le castigaría con 16 a 54 y cuatro meses de prisión, según el artículo 192 del Código Penal, el cual se refiere a quien “ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida una comunicación privada dirigida a otra persona, o se entere indebidamente de su contenido”; si la misma se divulga o se usa en provecho propio, la pena aumenta de 32a 72.

Por otro lado, el artículo 193 establece que se multará a quien “sin permiso de autoridad competente, ofrezca, venda o compre instrumentos aptos para interceptar la comunicación privada entre personas”. Cabe preguntarse si es aplicable esta sanción a la compañía Hacking Team o a los intermediarios que utiliza.

En la misma línea, la Ley 1273 de 2009 establece, en su artículo 269 A, una pena de c48 a 96 meses de cárcel a quien, sin autorización, “acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad” de la persona en cuestión. Por su parte, el artículo 269C establece de 36 a 72 meses de prisión a quien sin orden judicial previa “intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático”. El artículo 269E sanciona a quien “sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional *software* malicioso u otros programas de computación de efectos dañinos”. En este marco, es una agravante que el delito lo cometa un servidor público en ejercicio de sus funciones.

4.4. Ecuador

Mientras el Gobierno ecuatoriano ofrece asilo político a Julian Assange, líder de Wikileaks, y lo mantiene en su embajada en el Reino Unido⁸² también espía activamente a opositores

Policial con sus dependencias subordinadas, la cual dirigirá, coordinará e integrará la función de inteligencia y contrainteligencia en la Policía Nacional; b) Los grupos especializados de la Policía Nacional que sean creados por el Director General de la Policía Nacional, previo concepto de la Dirección de Inteligencia Policial, de acuerdo con su misión, competencias y funciones. 3. En el Departamento Administrativo “Dirección Nacional de Inteligencia, todas las dependencias orgánicas a ella. 4. En la Unidad de Información y Análisis Financiero (UIAF): todas las dependencias orgánicas a ella. <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=57315>

82 EFE. “Julian Assange Cumple Tres Años Recluido en la Embajada de Ecuador en Londres”. 20 minutos. 19 de junio

y activistas en su territorio a través de la Secretaría Nacional de Inteligencia (SENAIN). A mediados de junio de 2015, Hacking Team ofertó sus servicios al Ministerio del Interior. Esta institución requirió “un Centro Nacional de Monitoreo a nivel país”, que empezaría a funcionar en octubre de 2016.⁸³ En 2013, cuando se planteó la vigilancia masiva de comunicaciones en Ecuador, la Asamblea Nacional se pronunció sobre el tema indicando que “permitir a los prestadores de servicios de telecomunicaciones conserven información (...)específica sobre los usuarios, evidentemente podría traducirse en una transgresión al derecho a la intimidad”.⁸⁴

La contratación de la SENAIN se hizo a través de la empresa Theola Ltd., con sede en Belice, que a su vez es filial de Robotec Colombia. En total se gastaron 535 mil euros, más un mantenimiento de 75 mil euros al año.

Según Associated Press, de los correos filtrados surgen pruebas de que el gobierno de Rafael Correa utilizó el *malware* de Hacking Team para espiar a Carlos Figueroa, médico y activista político, quien en 2014 fue condenado a seis meses de prisión por “injurias” al presidente. La evidencia se encontraba en una serie de correos intercambiados entre Luis Solís, funcionario de SENAIN, y Bruno Muschitiello de Hacking Team, en el que discutían cómo enviar correos que sirvieran como gancho para instalar el *software* de espionaje en una dirección de correo que coincide con la de “dr.carlosfigueroa”.⁸⁵

Por otro lado, según un análisis técnico publicado en el blog del proyecto Tor, RCS también se utilizó contra organizaciones etiquetadas como Jueces, CNE, CONAIE - Pachakutks, El Creador y CJY Cia.⁸⁶ Estas organizaciones corresponderían a jueces, miembros del consejo nacional electoral, movimientos y partidos políticos alineados en la oposición al gobierno de Correa. Esto es problemático, pues las leyes ecuatorianas prohíben explícitamente el espionaje con fines políticos y no relacionados con la seguridad del país.

El 10 de julio de 2015, SENAIN negó tener relación contractual alguna con la compañía Hacking Team y aseguró que “es totalmente falso que alguna contratación de la SENAIN haya

de 2015. Consultado el 10 de noviembre de 2015. <http://www.20minutos.es/noticia/2493292/0/julian-assange/tres-anos/embajada-ecuador-londres/>

83 En un correo se responde textualmente desde Quito: “Hola Marco. Este es un nuevo grupo formado por el Ministerio del Interior (MDI) para ser usado por una serie de organismos activos en el ámbito policial. La atención está centrada en el tráfico de redes sociales. Como el MDI está detrás de esto, será la parte contratante”. Redacción Política. “Filtración a Hacking Team Revela Posible Espionaje a Escala Mundial”. El Comercio. 11 de julio de 2015. Consultado el 10 de noviembre de 2015. <http://www.elcomercio.com/actualidad/filtracion-hackingteam-ecuador-espionaje-mundial.html>.

84 Andrés Delgado. “Cámaras en los moteles: ‘Solo vigilamos los pasillos’”. 3 de marzo de 2015. Consultado el 10 de marzo de 2016. <http://andres.delgado.ec/2015/03/08/camaras-en-los-moteles-privacidad-ecuador-intimidad/>

85 Frank Bajak, and Raphael Satter. “Ecuador: Hacking The Opposition”. Associated Press. 7 de agosto de 2015. Consultado el 18 de septiembre de 2015. <http://bigstory.ap.org/article/6f41d49888174b45857d34511fda1caf/apnewsbreak-email-leak-suggests-ecuador-spied-opposition>

86 “Hacking Team, Chile y Ecuador”. People Tor Project. 11 de julio de 2015. Consultado el 16 de septiembre de 2015. https://people.torproject.org/~ilv/ht_chile_ecuador.html

servido para atacar medios digitales u otros objetivos políticos, como inescrupulosamente se está aseverando. Dicho esto, la Secretaría Nacional de Inteligencia se reserva el derecho legal de actuar en defensa de la seguridad nacional y del prestigio del Gobierno ecuatoriano”. El comunicado fue posteriormente removido y republicado como boletín de prensa en formato PDF.

Luego, miembros de la sociedad civil realizaron una petición a la comisión de fiscalización de la Asamblea Nacional para pedir transparencia sobre los procesos de Hacking Team. La Asamblea recibió al Secretario Nacional de Inteligencia, Rommy Vallejo, a puerta cerrada, tras lo cual no se hizo pública ninguna información. El Presidente Correa, en su informe semanal, defendió a la agencia de inteligencia e indicó que cada vez que se interceptan comunicaciones existe la presencia de miembros de la fiscalía, es decir que esto se estaría realizando sin la mediación de un juez.⁸⁷

Paradójicamente, Ecuador tiene una amplia regulación en cuanto a interceptación de datos, llamadas y mensajes. En todos los casos se exige una orden judicial y se prohíbe el espionaje con fines políticos. Sin embargo, la práctica parece distar mucho del panorama normativo.

Interceptación de comunicaciones privadas en un proceso penal

La regla general es que en toda interceptación de comunicaciones debe contarse con orden judicial. El Código Orgánico Integral Penal establece en el artículo 3.10 que “toda persona tiene derecho a su intimidad personal y familiar y no podrán hacerse registros, allanamientos, incautaciones en su domicilio, residencia o lugar de trabajo, sino en virtud de orden de la o el juzgador competente”. La Ley Orgánica de Telecomunicaciones prevé en su artículo 77 que únicamente se podrán realizar interceptaciones de datos y mensajes “cuando exista orden expresa de la o el juez competente, en el marco de una investigación de un delito o por razones de seguridad pública y del Estado, de conformidad con lo que establece la ley y siguiendo el debido proceso”.

Por otro lado, el artículo 470 del Código Orgánico Integral Penal establece que no se pueden grabar o registrar las comunicaciones personales de terceros sin que estos hayan conocido y autorizado dicha grabación o registro, salvo los casos expresamente señalados en la ley y con previa orden judicial.

En cuanto a la interceptación de comunicaciones en sentido estricto, el artículo 476 del Código Orgánico Integral Penal la permite, al igual que la interceptación de datos informáticos en el marco de un proceso judicial. El fiscal debe solicitar al juez la interceptación de cualquiera de las siguientes comunicaciones: telefonía fija, satelital, móvil e inalámbrica, con sus servicios de llamadas de voz, mensajes SMS, mensajes MMS, transmisión de datos y voz sobre IP, correo electrónico, redes sociales, videoconferencias y multimedia. Deben existir indicios suficientes que prueben su valor, de otra manera no podrá hacerse. El plazo de interceptación no puede ser mayor a 90 días prorrogables una sola vez. Tratándose de investigaciones de delincuencia organizada y sus delitos relacionados, la interceptación

87 Fundamedios. “Senain Advierte con Tomar Acciones Legales por Divulgar Información que la Relacionan con Hacking Team”. 16 de julio de 2015. Consultado el 10 de octubre de 2016. <http://www.fundamedios.org/alertas/senain-advierde-con-tomar-acciones-legales-por-divulgar-informacion-que-la-relacionan-con-hacking-team/>

podrá realizarse hasta por un plazo de seis meses prorrogables. Todo lo que se intercepte debe ser guardado en secreto.

No se pueden interceptar las comunicaciones protegidas por secretos profesionales y religiosos; tampoco las comunicaciones que vulneren los derechos de los niños, niñas y adolescentes o en aquellos casos que generen la revictimización de mujeres víctimas de violencia.

El problema con RCS es que no hay manera de garantizar el control y la discriminación de este tipo de comunicaciones no interceptables si se tiene control del dispositivo completo.

Por último, según los artículos 476 y 528 del Código Orgánico Integral Penal, si durante la interceptación de llamadas se descubre la comisión de un delito distinto al investigado, se puede arrestar al sospechoso en el instante.

Incautación de objetos

Si el artículo 478 del Código Orgánico Integral Penal se refiere a una incautación física, podría aplicarse de manera análoga sus requisitos, pues RCS toma control de computadoras y celulares para permitir que se inspeccione y observe todo lo que está dentro de los mismos. Para el registro tanto de personas como de objetos que tengan relación con el delito, se necesitaría la autorización de la persona afectada o una orden judicial. En este último caso deberá ser motivada y debe limitarse a lo señalado en la misma. Es decir, no se puede inspeccionar todo. Esto presenta también un problema, pues, como ya hemos mencionado, RCS toma control de todo el dispositivo sin que se puedan limitar las actividades del *software*.

Interceptación de comunicaciones por agencias de inteligencia

La Ley de Seguridad Pública y del Estado define las actividades de inteligencia en su artículo 14 como “la actividad consistente en la obtención, sistematización y análisis de la información específica referida a las amenazas, riesgos y conflictos que afecten a la seguridad integral”. Esta información de inteligencia es sustancial para la toma de decisiones en materia de seguridad.

Sin embargo, de acuerdo al artículo 20, si los organismos de inteligencia (incluyendo a la SENAIN) necesitan “retener, abrir, interceptar o examinar documentos o comunicaciones por cualquier medio”, deben solicitar una orden judicial al Presidente o Presidenta de la Corte Nacional de Justicia. Dicha interceptación puede concederse hasta por un plazo máximo de 60 días prorrogables.

Vale la pena mencionar que según el artículo 20 de la Ley de Seguridad Pública y del Estado, e necesita de una autorización judicial para llevar a cabo este tipo de interceptación de comunicaciones. Este mismo juez podrá negar la solicitud por “afectación grave a los derechos de los sujetos sobre quienes se ejerce la operación encubierta, o por considerar que tiene como único objetivo el beneficio político del requirente”.

Además de que el espionaje con fines políticos es ilegal, el artículo 22 es muy claro al estable-

cer que está prohibido obtener información, producir inteligencia o almacenar datos sobre personas en razón de “etnia, orientación sexual, credo religioso, acciones privadas, posición política o de adhesión o pertenencia a organizaciones partidarias”. En otras palabras: la instalación del *software* de Hacking Team a miembros de la oposición política no solo es ilegal por falta de autorización, sino también por infracción de una prohibición expresa.

Sanciones

El artículo 178 del Código Orgánico Integral Penal establece de uno a tres años de prisión para la persona que “sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio”. Es decir, que si se utilizó el programa de Hacking Team sin orden judicial, los funcionarios que lo hicieron deberían ir a prisión conforme a las leyes ecuatorianas.

Además, el artículo 230 del Código establece una sanción de tres a cinco años de prisión para quien “diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder” y la misma pena a la persona que “produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos” destinados a la comisión de dichos delitos. Bajo este supuesto, cabe preguntarnos si la empresa de Hacking Team sería castigada bajo leyes ecuatorianas.

4.5. Honduras

El Gobierno hondureño empezó a negociar con Hacking Team en 2012. Dos años después, la Dirección Nacional de Investigación e Inteligencia (DNII) compró Galileo.⁸⁸ La compañía israelí NICE Systems actuó como intermediario vía Ori Zoller, un ex militar israelí dedicado a la venta de armas AK-47 que eventualmente terminaron en manos de grupos paramilitares en Colombia.⁸⁹ En total se gastaron 355 mil euros.

En Honduras se regula la interceptación de comunicaciones siempre y cuando exista orden judicial y se respeten los principios de proporcionalidad, necesidad, idoneidad, confidencialidad, reserva jurisdiccional y temporalidad. A pesar de que la regulación es amplia y se apeg a estándares de derechos humanos, el resto de atribuciones y capacidades de RCS no están reguladas, por lo que se presenta un problema de legalidad.

88 Elizabeth Gonzalez. “Explainer: Hacking Team’s Reach in the Americas”. Americas Society Council of the Americas. 30 de Julio de 2015. Consultado el 10 de octubre de 2015. <http://www.as-coa.org/articles/explainer-hacking-teams-reach-americas-0>

89 Lee Fang. “Former AK-47 Dealer Goes Cyber, Supplied Surveillance Tools to Honduras Government”. The Intercept. July 27, 2015. Accessed March 09, 2016. <https://theintercept.com/2015/07/27/ak-47-arms-dealer-goes-cyber-supplied-surveillance-tools-honduras-government/>

Interceptación de comunicaciones en procesos penales

El artículo 100 de la Constitución establece la regla general de orden judicial, estableciendo que “toda persona tiene derecho a la inviolabilidad y al secreto de las comunicaciones (...) salvo resolución judicial”. Por otro lado, la Ley Marco del Sector de Telecomunicaciones establece en su artículo 3 que las telecomunicaciones son inviolables y por tanto no pueden “ser interceptadas o interferidas, salvo por resolución judicial”.

Según las leyes hondureñas, una comunicación privada es la que se realiza entre emisor y receptor, revestida de privacidad y que solamente interesa a los interlocutores o cuando se celebre dentro un ámbito estrictamente doméstico, no integrado o conectado a una red de difusión de cualquier tipo. Por otro lado, la interceptación de comunicaciones es una técnica especial de investigación mediante la cual “se escucha, capta, registra, guarda, graba y observa por parte de la autoridad, sin el consentimiento de sus titulares, una comunicación” de cualquier tipo.

La Ley Especial sobre Interceptación de Comunicaciones Privadas establece que, para hacerse, se deben obedecer los principios de proporcionalidad, necesidad e idoneidad, confidencialidad, reserva jurisdiccional y temporalidad (artículo 5). Las autoridades facultadas para pedirla ante el juez son el Ministerio Público, la Policía Nacional y la Procuraduría General de la República en un principio (artículo 7) y debe recaer sobre las comunicaciones y medios de soporte físicos o virtuales que utilicen las personas investigadas (artículo 10). Están prohibidas las interceptaciones de las comunicaciones entre el abogado defensor y los imputados (artículo 11).

El contenido de la solicitud al juez debe plantearse por escrito y tener a) el nombre y apellido de las personas b) la descripción de los hechos y delitos que se investigan c) los datos de identificación del servicio de comunicación a interceptar (artículo 15). El juez tiene 4 horas para considerar la gravedad del delito investigado y la utilidad, necesidad, idoneidad y proporcionalidad de la medida para poder otorgarla (artículo 16). Este procedimiento y toda la interceptación en su totalidad será reservado. Solo el juez de garantía, el fiscal o agente de la Procuraduría General de la República tienen acceso a la misma (artículo 26). No puede durar más de tres meses, aunque esto es prorrogable hasta por tres periodos más (artículo 32).

El organismo responsable de ejecutar la interceptación es la Unidad de Interceptación de las Comunicaciones y debe respetar los criterios anteriores (artículos 23 y 33).

Como contexto, hay que mencionar que las compañías que brindan servicios de comunicación y telefonía tienen la obligación de registrar a sus clientes e identificarlos, además de guardar todo tipo de metadatos relacionados con sus comunicaciones por un periodo de cinco años (artículo 39).

Además, si en cualquier punto de la investigación los Fiscales tienen en su poder pruebas que fueron obtenidas por medios ilícitos o violaciones de derechos humanos, no podrán utilizarlas en un juicio. Esto implica que si no se respeta el requisito de la orden judicial y se

utiliza el *software* de Hacking Team para obtener pruebas contra una persona, las mismas deben desecharse (artículo 94 del Código Procesal Penal).

Interceptación de comunicaciones por agencias de inteligencia

El artículo 2 de la Ley de Inteligencia Nacional faculta a la Dirección Nacional de Investigación e Inteligencia –la entidad hondureña que compró el *software* de espionaje de Hacking Team– para “desarrollar actividades de investigación e inteligencia estratégica para proteger los derechos y libertades de los ciudadanos y residentes en el país (y) prevenir y contrarrestar amenazas internas o externas contra el orden constitucional”. El artículo 9 establece que dentro de las funciones de este organismo se encuentra la de desarrollar actividades de investigación e inteligencia estratégica con el fin de a) identificar y contrarrestar actividades que puedan representar una amenaza para la seguridad y el desarrollo nacional y b) desarrollar actividades de investigación e inteligencia en cooperación con los demás organismos de inteligencia nacional, así como con otras entidades del Estado.

El supuesto es tan amplio y tan dedicado a los objetivos en lugar de los mecanismos de obtención de los mismos, que en teoría podría incluir al *software* de espionaje de Hacking Team. No existen disposiciones específicas sobre la interceptación de comunicaciones ni sobre la interceptación de equipos.

Sanciones

Si se llegara a utilizar el *software* de Hacking Team sin autorización judicial, los artículos 48 y 49 de la Ley Especial sobre interceptación de las Comunicaciones Privadas establecen las penas de prisión entre 4 y 19 años a los funcionarios públicos o empresas que divulguen la información interceptada o altere el contenido de la interceptación de las comunicaciones. A la fecha, ninguna investigación se ha abierto.

4.6. México

Según la Comisión Interamericana de Derechos Humanos en su informe “Situación de derechos humanos en México”, este país atraviesa una grave crisis.⁹⁰ En un contexto marcado por desapariciones forzadas, ejecuciones extrajudiciales, tortura, impunidad y violencia contra periodistas, el Gobierno mexicano aparece además como el cliente más importante de Hacking Team a nivel mundial, gastando un total de €5.808.875 por la compra de más de 15 licencias de espionaje.⁹¹ La empresa que funcionó como intermediaria en las negociaciones fue SYM Servicios Integrales.

Varias dependencias realizaron esta compra: el Centro de Investigación y Seguridad Na-

90 Comunicado De Prensa. “CIDH Publica Informe sobre la Situación de Derechos Humanos en México”. Organización de los Estados Americanos. 2 de marzo de 2016. Consultado el 10 de marzo de 2016. <https://www.oas.org/es/cidh/prensa/Comunicados/2016/023.asp>

91 Arturo Angel. “México, el principal cliente de una empresa que vende software para espiar”. Animal Político. 7 de Julio de 2015. Consultado el 19 de octubre de 2015. <http://www.animalpolitico.com/2015/07/empresa-de-hackers-exhibida-por-venta-de-software-espia-a-paises-represores-y-mexico-resulta-su-principal-cliente/>

cional; la Procuraduría General de Justicia y los Cuerpos de Seguridad Auxiliar del Estado de México; la Secretaría de Seguridad Pública de Tamaulipas; la Secretaría de Planeación y Finanzas de Baja California; la Policía Federal; la Secretaría de Marina; Petróleos Mexicanos (PEMEX) y los estados de Jalisco, Querétaro, Puebla, Campeche y Yucatán.⁹²

Tan solo el organismo de inteligencia, CISEN, pidió 2.074 permisos judiciales para utilizar este *software*.⁹³ Concretamente, en el estado de Puebla, el Gobierno utilizó las herramientas de Hacking Team para espiar a oponentes políticos y periodistas. Primero, al vigilar la casa de campaña de un político de oposición llamado Ernesto Cordero y después a diversos periodistas a quienes enviaron correos engañosos para poder inocular sus aparatos.⁹⁴

El 7 de julio, cuando la prensa cuestionó al Secretario de Gobernación Miguel Ángel Osorio Chong respecto a la compra del *software* de espionaje, el funcionario respondió que había sido comprado por la administración pasada. Es decir, por otro partido en el periodo del presidente anterior.⁹⁵ Por otro lado, los gobiernos de los estados de Jalisco, Yucatán, Durango y Campeche negaron toda relación con dicha empresa de espionaje.⁹⁶ Ambas afirmaciones resultaron ser falsas.

En México existen salvaguardas constitucionales amplias en cuanto a la interceptación de comunicaciones privadas.⁹⁷ La Constitución y las leyes exigen el requisito de orden judicial y prohíben que autoridades estatales las realicen. En este sentido, el problema radica más en la aplicación de la ley que en su redacción misma. Sin embargo, y como es una tendencia en la región, otras actividades como la geolocalización o incautación no están reguladas de acuerdo a parámetros aceptables en términos de derechos humanos.

Como regla general, el artículo 16 de la Constitución Federal establece que las comunicaciones privadas son inviolables y que “exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la

92 Ídem

93 Mauricio Romero. “Cisen: 2 mil 74 solicitudes para espiar con tecnología de Hacking Team”. Contralínea. 6 de marzo de 2016. Consultado el 10 de marzo de 2016. <http://www.contralinea.com.mx/archivo-revista/index.php/2016/03/06/cisen-2-mil-74-solicitudes-para-espiar-con-tecnologia-de-hacking-team/>

94 Ernesto Aroche. “El gobierno de Puebla usó el software de Hacking Team para espionaje político”. Animal Político. 22 de julio de 2015. Consultado el 19 de octubre de 2015. <http://www.animalpolitico.com/2015/07/el-gobierno-de-puebla-uso-el-software-de-hacking-team-para-espionaje-politico/>

95 Redacción. “Osorio Chong dice que México compró software a Hacking Team en el gobierno de Calderón”. Sin Embargo. 7 de Julio de 2015. Consultado el 18 de septiembre de 2015. <http://www.sinembargo.mx/07-07-2015/1405444>

96 Redacción. “Acusa R3D a Jalisco de comprar programa espía a ‘Hacking Team’”. Aristegui Noticias. 9 de Julio de 2015. Consultado el 18 de septiembre de 2015. <http://aristeginoticias.com/0907/mexico/acusa-r3d-a-jalisco-de-comprar-programa-espia-a-hacking-team/>

97 Luis Fernando García. “Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en México”. Electronic Frontier Foundation. Octubre de 2015. Consultado el 19 de diciembre de 2015. <https://www.eff.org/node/89090>

entidad federativa correspondiente, podrá autorizar la interceptación de cualquier comunicación privada”. Se prohíbe en materia electoral, fiscal, mercantil, civil, laboral o administrativo, así como en el caso de las comunicaciones del detenido con su defensor.

Cuando pensamos en el *software* de Hacking Team, la regla constitucional parece traer dos problemas específicos. Primero, porque no hay manera de ejercer un control sobre las materias y tipo de conversaciones que se graban e interceptan: RCS tiene acceso a prácticamente todo, lo cual abre la puerta a abusos. La segunda, porque si la Constitución establece que solo las autoridades federales con facultades legales o los Ministerios Públicos estatales pueden pedir al juez la interceptación de comunicaciones, el *software* comprado por los estados de Jalisco, Querétaro, Puebla, Campeche y Yucatán es ilegal, pues fueron las Secretarías de Gobierno quienes lo adquirieron sin facultades debidas para hacerlo. Según Luis Fernando García de R3D, las únicas autoridades facultadas son la Procuraduría General de la República, las Procuradurías Estatales, la Policía Federal y el CISEN.

De la misma forma, Petróleos Mexicanos es una empresa del Estado que se dedica a la explotación de los recursos energéticos (principalmente petróleo y gas natural) en territorio mexicano y tampoco tiene facultades para interceptar comunicaciones o incautar computadoras y celulares.⁹⁸

Interceptación de comunicaciones privadas en un proceso judicial

En cuanto a autoridades facultadas, el artículo 291 del Código Nacional de Procedimientos Penales establece que, en el marco de una investigación, tanto la Procuraduría General de la República y los Procuradores de los estados podrán solicitar al juez una autorización para la misma.

El supuesto incluye prácticamente todo el contenido de una computadora o celular que puede ser accedido por el programa de Hacking Team pues dice literalmente “todo un sistema de comunicación o programas que sean fruto de la evolución tecnológica, que permitan el intercambio de datos, informaciones, audio, video, mensajes, así como archivos electrónicos, que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación, las cuales se pueden presentar en tiempo real o con posterioridad al momento en que se produce el proceso comunicativo”.

Sin embargo, los servidores públicos que ejecuten la medida serán responsables de que se realice en los términos de la resolución judicial. No pueden ser interceptadas las comunicaciones electorales, fiscales, mercantiles, civiles, laborales o administrativas, ni tampoco las comunicaciones del detenido con su defensor. El artículo 295 establece que si en la interceptación se tiene conocimiento de un delito diverso de aquellos que motivan la medida, se iniciará una nueva investigación. Según el artículo 300, los registros que no tengan relación con el objeto del delito deben ser eliminados; el *software* de Hacking Team los conserva.

98 Reglamento de la Ley Orgánica de Petróleos Mexicanos. Publicado el 10 de Agosto de 1972. Consultado el 18 de diciembre de 2015. http://www.pemex.com/acerca/marco_normativo/Documents/reglamentos/REG_LEY_ORGANICA_PEMEX.pdf

Por otro lado, si se usa el *software* de Hacking Team sin orden judicial y de ahí se obtienen pruebas en contra de una persona, las mismas no pueden ser usadas según el artículo 264 del Código Nacional de Procedimientos Penales, que considera como prueba ilícita cualquier cosa que se obtenga violando derechos humanos.

Geolocalización

En cuanto a la localización geográfica de personas a partir de sus teléfonos celulares o computadoras, el artículo 303 del Código Nacional de Procedimientos Penales prevé que, en el marco de una investigación, el procurador puede pedir a los concesionarios, permisionarios o comercializadoras del servicio de telecomunicaciones o comunicación vía satélite los datos sobre los mismos. Los artículos 189 y 190 de la Ley Federal de Telecomunicaciones y Radiodifusión tienen una disposición similar, pues obligan a los proveedores de servicio de internet a colaborar “con las instancias de seguridad, procuración y administración de justicia, en la localización geográfica, en tiempo real, de los equipos de comunicación móvil”.

Es dudoso que estas reglas sean aplicables al *software* de Hacking Team, pues ambas leyes se refieren a pedir los datos de geolocalización a los proveedores de servicios de internet o comunicación, mientras que RCS los obtiene directamente de la computadora o teléfono celular de la persona inoculada. En última instancia, lo que esto implica son menos controles sobre la información de los usuarios.

Incautación de objetos

Por otro lado, los artículos 229 a 234 del Código Nacional de Procedimientos Penales establecen las reglas para el aseguramiento de bienes, instrumentos u objetos relacionados con actividades delictivas en el marco de una investigación. Se deben establecer controles específicos para su resguardo y hacer un inventario de los mismos. Además, el artículo 267 del mismo ordenamiento prevé la inspección de objetos sobre “todo aquello que pueda ser directamente apreciado por los sentidos”. Este último supuesto podría utilizarse para legitimar las prácticas derivadas del programa de espionaje de Hacking Team.

Interceptación de comunicaciones por agencias de inteligencia

En cuanto a la interceptación de comunicaciones fuera de procesos judiciales, el artículo 13 de la Ley de Seguridad Nacional faculta al Consejo de Seguridad Nacional emitir “los lineamientos para regular el uso de aparatos útiles en la interceptación de comunicaciones privadas”. A la fecha aún no se ha emitido ningún documento al respecto.

Se entiende por interceptación de comunicaciones la toma, escucha, monitoreo, grabación o registro de comunicaciones privadas de cualquier tipo y por cualquier medio, aparato o tecnología. Es importante resaltar que únicamente es procedente contra las siguientes amenazas a la seguridad nacional: a) actos de espionaje, sabotaje, terrorismo, rebelión, traición a la patria o genocidio b) actos que impidan a las autoridades actuar contra la delincuencia organizada c) actos que atenten en contra del personal diplomático d) financiamiento de organizaciones terroristas, etc. Es decir que si se utiliza el *software* de Hacking

Team para interceptar comunicaciones privadas de cualquier tipo con objetivos distintos, estas son ilegales.

Si bien por esta ley CISEN tiene facultades para interceptar comunicaciones privadas, el artículo 34 establece que, para efectuarlas, se deberá solicitar la correspondiente autorización judicial. Por otro lado, el artículo 28 establece que la solicitud que el CISEN haga a los jueces debe contener una descripción detallada de los hechos que representen alguna amenaza para la seguridad nacional y la duración de la autorización que se solicita. No hay forma de saber si CISEN ha cumplido con estas reglas, pues el artículo 45 establece que el personal del juzgado está obligado a mantener secreto del contenido de las solicitudes y resoluciones de autorización, así como aquella información generada por la aplicación de las mismas.

Adicionalmente, la Ley Federal de Delincuencia Organizada regula la interceptación de comunicaciones en casos de narcotráfico o delincuencia organizada. Su artículo 8 establece que la Procuraduría General de la República debe contar con una unidad especializada en la investigación y persecución de delitos cometidos por miembros de la misma.⁹⁹ Esta unidad debe contar con un cuerpo técnico de control, que en las interceptaciones de comunicaciones privadas verificará la autenticidad de sus resultados y establecerá lineamientos sobre las características de los aparatos, equipos y sistemas.

Los artículos 16 a 26 regulan detalladamente el procedimiento de interceptación de dichas comunicaciones. Primero si, antes del proceso, durante la investigación previa de un delito relacionado con la delincuencia organizada, se tienen que interceptar comunicaciones, el Procurador o el titular de la “unidad especializada” lo deben solicitar por escrito al juez expresando los detalles de la misma (artículo 16).

Esta petición debe resolverse dentro de las doce horas siguientes a que sea recibida la solicitud, pero en ningún caso podrá autorizar interceptaciones en materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor (artículo 17).

La interceptación la puede llevar a cabo únicamente el Ministerio Público. La autorización judicial debe señalar las comunicaciones que serán escuchadas o interceptadas; los lugares que serán vigilados y el periodo durante el cual se llevarán a cabo las interceptaciones, el que podrá ser prorrogado sin exceder seis meses (artículo 19). Una vez más, se reitera que las interceptaciones realizadas sin las autorizaciones antes citadas o fuera de los términos ordenados carecerán de valor probatorio. (artículo 19)

Por otro lado, el Ministerio Público debe levantar un acta circunstanciada con las fechas de inicio y término de la interceptación; un inventario pormenorizado de los documentos, objetos y las cintas de audio o video que contengan los sonidos o imágenes captadas durante la misma; la identificación de quienes hayan participado en las diligencias, así como los demás datos que considere relevantes para la investigación (artículo 22). Esto último es

99 Agentes del Ministerio Público de la Federación, auxiliados por agentes de la Policía Judicial Federal y peritos.

muy importante de cara al *software* de espionaje de Hacking Team, pues este registro permitiría ejercer un control posterior sobre la vigilancia del programa en caso de violaciones a derechos humanos.

Sin embargo, todas las reglas anteriores se refieren a procedimientos de interceptación de comunicaciones, distintos de las capacidades de apoderamiento y control a distancia de equipos e historiales que permite RCS. En tal sentido, resulta muy cuestionable que estas reglas permitan el uso lícito del *software* de Hacking Team.

Sanciones

En caso de que no se sigan los requisitos que las leyes establecen, el artículo 27 de la Ley Federal de Delincuencia Organizada prevé una pena de prisión de seis a doce años y destitución e inhabilitación a cualquier servidor público que intervenga comunicaciones privadas sin la autorización judicial correspondiente o en términos distintos a lo que establece la orden judicial. El artículo 28 prevé la misma pena para el servidor que divulgue la información. Además, el Código Penal Federal prevé 180 jornadas de trabajo a favor de la comunidad a quien indebidamente intercepte una comunicación escrita que no esté dirigida a él; y de seis a 12 años de prisión a quien intervenga comunicaciones privadas sin orden judicial.

4.7. Panamá

En Panamá existen antecedentes de espionaje respecto a un programa llamado Pegasus, comprado por la oficina del ex presidente Ricardo Martinelli.¹⁰⁰ La Corte Suprema de Justicia lo acusó y procesó por interceptar las comunicaciones de 150 personas entre empresarios, periodistas, dirigentes de la sociedad civil y políticos opositores a su gobierno.¹⁰¹ En este mismo contexto, el Consejo de Seguridad Nacional presentó en enero de 2015 una querrela contra Julio Moltó, Gustavo Pérez y Alejandro Garuz, tres ex funcionarios de este organismo implicados en las escuchas telefónicas.

En lo que concierne a Hacking Team, la Oficina de Seguridad de la Presidencia de Panamá adquirió el software Galileo a través de la empresa intermediaria Robotec Colombia en 2011. En Panamá, esta empresa creó una subsidiaria representada por Michael Schwartz y Teófilo Homsany.¹⁰²

Según los correos, el entonces presidente Martinelli estaba al tanto de las negociaciones

¹⁰⁰ Carlos Alberto Vargas. “Escuchas ilegales en el gobierno anterior. Triangularon compra de equipo para espionaje”. La Prensa Panamá. 27 de julio de 2015. Consultado el 19 de septiembre de 2015. http://www.prensa.com/politica/Triangularon-compra-equipo-espionaje_O_4264823642.html

¹⁰¹ Agencia AFP. “Corte Suprema de Panamá ordena detención de expresidente Martinelli”. Diario El Telégrafo. 22 de diciembre de 2015. Consultado el 23 de diciembre de 2015. <http://www.eltelegrafo.com.ec/noticias/mundo/9/corte-suprema-de-panama-ordena-detencion-de-expresidente-martinelli>

¹⁰² Redacción de la Prensa. “10 claves para entender el caso de Hacking Team en Panamá”. La Prensa. 11 de julio de 2015. Consultado el 9 de agosto de 2015. http://www.prensa.com/politica/claves-entender-Hacking-Team-Panama_O_4251324994.html#sthash.ljlzx37N.dpuf

cuando Robotec se reunió con su “cliente... el Sr. Adolfo De Obarrio, secretario privado del Presidente de Panamá”. Si bien Martinelli no estaba presente, sí estaba al teléfono durante el tiempo completo¹⁰³ y tenía interés en espiar a 40 perfiles específicos.¹⁰⁴

El contrato vencía el 31 de mayo de 2014.¹⁰⁵ Sin embargo, poco tiempo después de las elecciones y antes de que el nuevo presidente tomara posesión de su cargo, el equipo de espionaje de Panamá se perdió.¹⁰⁶ La plataforma de espionaje estuvo transmitiendo los datos, chats y otras informaciones de sus víctimas hasta pasadas dichas elecciones. En total, el Gobierno panameño gastó 750 mil euros.

Ante esto, la Fiscalía Primera Anticorrupción de Panamá inició una averiguación por la compra y posterior desaparición de los equipos de espionaje adquiridos por el Gobierno de Martinelli a la compañía italiana Hacking Team.¹⁰⁷

El *software* de espionaje fue utilizado para inocular a Carlos Arjona, Director de Informática en el Ministerio de la Presidencia de julio de 2009 a julio de 2011, y salió por oponerse a la compra y negociaciones con Hacking Team.¹⁰⁸

En Panamá, la regulación de interceptación de comunicaciones es lo suficientemente amplia para abarcar también otras actividades del *software* de Hacking Team. Sin embargo, siempre se requiere de una orden judicial y se prohíbe el espionaje hecho con fines políticos.

Interceptación de comunicaciones en un proceso judicial

La regla general, según el artículo 29 de la Constitución, es que toda correspondencia, documentos y comunicaciones privadas son inviolables y no podrán ser interceptadas, registradas o grabadas sin orden judicial y con fines específicos. Lo contrario implica que

103 Vince@hackingteam.com. “Status Solution RCS Panama”. E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/600077>

104 Elizabeth González. “Explainer: Hacking Team’s Reach in the Americas”. Americas Society Council of the Americas. 30 de Julio de 2015. Consultado el 15 de septiembre de 2015. <http://www.as-coa.org/articles/explainer-hacking-teams-reach-americas-O>

105 “La Empresa Hacking Team fue infiltrada y entre sus clients Panamá”. Algo Más Duro. 7 de Julio de 2015. Consultado el 14 de octubre de 2015. <http://www.algomasduro.com/inicio/tecnologia/39335-la-empresa-hacking-team-fue-infiltrada-y-entre-sus-clientes-panama>

106 Rolando Rodríguez, y Juan Manuel Díaz. “Abren sumario en caso Hacking Team”. La Prensa Panamá. 7 de agosto de 2015. Consultado el 16 de octubre de 2015. http://www.prensa.com/locales/Espiar-obsesion-Martinelli_O_4271572998.html y Lorenzo Franceschi-Biccieri. “Hacking Team’s Equipment Got Stolen in Panama”. Motherboard VICE. 7 de julio de 2015. Consultado el 4 de agosto de 2015. <https://motherboard.vice.com/read/hacking-teams-equipment-got-stolen-in-panama>

107 Tabatha Molina. “Panamá pesquisa gestión de Martinelli por caso Hacking Team”. Panam Post. 10 de agosto de 2015. Consultado el 14 de agosto de 2015. <http://es.panampost.com/thabata-molina/2015/08/10/panama-investigara-a-martinelli-porescandalo-de-hacking-team/>

108 Rolando Rodríguez, y Juan Manuel Díaz. “Abren sumario en caso Hacking Team”. La Prensa Panamá. 7 de agosto de 2015. Consultado el 16 de octubre de 2015. http://www.prensa.com/locales/Espiar-obsesion-Martinelli_O_4271572998.html

la información que se obtenga no se puede usar como prueba, además de las responsabilidades penales en las que incurren quienes la obtengan. Los artículos 379 y 381 del Código Procesal Penal, refuerzan esta idea, pues los elementos de prueba solo pueden ser valorados si han sido obtenidos por medios legales y no violan derechos humanos.

En otras palabras, si con la intrusión de *software* de espionaje de Hacking Team se obtiene información que podría ser utilizada como prueba en un juicio, las mismas deben ser desechadas si no usa el programa con orden judicial, violando el derecho humano a la privacidad o intimidad.

En el marco de procesos judiciales, la “intercepción o grabación de comunicaciones personales por cualquier medio técnico” se regula en el artículo 311 del Código Procesal Penal, mismo que establece la necesidad de una autorización judicial a petición del Fiscal. Ciertas actividades facilitadas por el *software* de Hacking Team –incluyendo la geolocalización de personas– estarían comprendidas por este artículo, pues el mismo abarca “comunicaciones cibernéticas, seguimientos satelitales, vigilancia electrónica y comunicaciones telefónicas”. No obstante, es difícil calificar como legal el uso del mecanismo de *malware* como forma de ejecución de esas medidas.

Por otro lado, el artículo 310 establece que para interceptar correspondencia o documentos privados también se necesita una autorización judicial previa; y el artículo 264 del mismo ordenamiento prevé que el juez puede autorizar el secuestro de cartas, pliegos, paquetes, valores, telegramas u otros objetos de correspondencia cuando existan razones fundadas para suponer que les han sido dirigidos al imputado y estén relacionadas con el delito.

Si se autoriza la interceptación, no puede exceder de 20 días y solo podrá ser prorrogado si así lo pide el Ministerio Público. El funcionario de gobierno que ejecute la orden tiene la obligación de guardar secreto sobre su contenido, salvo que sea citado como testigo en un proceso. Si se guarda y conserva el material en un medio digital, el mismo deberá permanecer guardado bajo una cadena de custodia.

Incautación de objetos y equipos informáticos

El artículo 314 del Código Procesal Penal establece las reglas para la incautación (o apoderamiento) de datos en equipos informáticos. Le aplican los mismos límites referidos al secreto profesional y a la reserva sobre el contenido de los documentos incautados. Si el contenido debiera examinarse, se citará a la persona procesada y su abogado para hacerlo. El artículo 308 establece que cualquier otro bien empleado en la comisión de un delito también puede ser tomado por el Ministerio Público y además se pueden apoderar de “copias, reproducciones o imágenes de objetos” cuando sea conveniente.

Podría hacerse una analogía legal que aplicase ambos conceptos al *software* de espionaje de Hacking Team, aunque no se trata de apoderamiento físico de computadoras y celulares, el efecto es el mismo pues se puede leer, analizar y copiar la información dentro de estos aparatos.

El artículo 309 establece que no podrán ser objeto de incautación las comunicaciones escritas y notas entre el acusado y su abogado, o de las personas que puedan excusarse de declarar como testigos; tampoco los resultados de exámenes o diagnósticos médicos. Con el programa de espionaje de Hacking Team no hay manera de hacer respetar la información reservada o estrictamente privada contra injerencias de la autoridad, pues se tiene acceso a prácticamente todo.

Intercepción de comunicaciones por agencias de inteligencia

En cuanto a los procesos de espionaje fuera de procesos judiciales, en 2010 se derogó la Ley de 20 de agosto de 2008 que había creado el Consejo de Seguridad Pública y Defensa Nacional: integrado por el Ministro de Gobierno y Justicia, el canciller, el Ministro de Economía y Finanzas y el Presidente de la República. En su lugar, el Decreto Ejecutivo 263 del 19 de marzo de 2010 crea el Consejo de Seguridad Nacional actual: un organismo consultivo y asesor del Presidente en materia de seguridad pública y defensa, integrado por el Ministro de la Presidencia y el propio Presidente.

Este Consejo cuenta con una Secretaría, cuyos miembros son de libre nombramiento y remoción por el Presidente de dicho país.

El artículo 13.5 prohíbe explícitamente “la realización de actividades que involucren espionaje político”. Por otro lado, según el artículo 15, esta Secretaría adscrita al Presidente tiene entre sus funciones “realizar las tareas de inteligencia que contribuyan a preservar la integridad, estabilidad y permanencia de la República de Panamá” y además “investigar, preparar y recabar la información necesaria para alertar y prevenir los riesgos y amenazas a la seguridad nacional”. La definición no incluye la interceptación de comunicaciones de manera explícita.

Aunque la Constitución lo establece, el Decreto Presidencial que regula a este organismo de inteligencia no menciona el requisito de orden judicial previa para realizar labores de espionaje. Por otro lado, es difícil tener un control y fiscalización de estas actividades, pues el artículo 7 del mismo Decreto establece la clasificación de información de acceso restringido de las actividades de la Secretaría y el Consejo. Igualmente, en la Ley 6 de 2002 artículo 29, se señala que ese tipo de información es prohibida de acceso público, por ser de interés de seguridad nacional del Estado.

Sanciones

Por último, si no se siguen estas reglas se castiga con dos a cuatro años de prisión a quien sin autorización judicial “intercepte telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción de conversaciones no dirigidas al público”, según el artículo 167 del Código Penal de Panamá. Lo mismo a quien “sustraiga, destruya, sustituya, oculte, extravíe, intercepte o bloquee una carta, pliego, correo electrónico, despacho cablegráfico o de otra naturaleza, dirigidos a otras personas”, según el artículo 165 del mismo Código. La pena aumenta de tres a cinco años de prisión si la persona es servidor público o empleado de alguna empresa de telecomu-

nicación. Por otro lado, el artículo 166 sanciona con 200 a 500 días de multa o arresto de fines de semana a quien haga públicos correspondencias o grabaciones personales.

5. Otros países que negociaron con Hacking Team

5.1. Argentina¹⁰⁹

La primera vez que el Gobierno argentino contactó a Hacking Team fue en marzo de 2012, cuando Alex Velasco (el encargado de la actividad de la empresa en América Latina) organizó una visita a Buenos Aires para realizar una demostración de Remote Control System en varios lugares del país. Según los correos,¹¹⁰ se realizaron seis demostraciones entre el 19 y el 23 de marzo de 2012, con la presencia de autoridades del Ministerio de Seguridad de la Nación, la Dirección Nacional de Inteligencia Criminal, el Ministerio Público Fiscal,¹¹¹ la Unidad de Investigaciones Complejas y el Ministerio de Justicia y Seguridad de la Provincia de Buenos Aires.

En años posteriores, cuatro distintas empresas hicieron contacto con Hacking Team sin concretar ninguna venta específica.

En primer lugar, Nullcode Team en 2014, a quien Hacking Team respondió que únicamente vendían sus productos a agencias de seguridad y entidades gubernamentales y no de manera directa a empresas privadas.¹¹²

El encargado de llevar adelante las conversaciones en Argentina fue Mariano Russo, entonces director de la empresa, quien se presentó ante Hacking Team con conexiones en ese país, en Perú y en Bolivia, y dispuesto a ofrecerle a sus contactos en esos Estados el *software* de la empresa italiana. Otro representante de Nullcode, además, confirmó que la empresa no trabajaba con compañías privadas, sino que solo ofrecía su servicio a gobiernos.

La respuesta del representante de Hacking Team fue más allá y le expresó a Russo que,

109 Crédito general de Leandro Uciferri. "Hacking Team y sus planes para hackear en Argentina". Tecnovortex. 10 de julio de 2015. Consultado el 18 de octubre de 2015. <http://tecnovortex.com/hacking-team-argentina/>

110 Aскарfile@hackingteam.it. "Argentina". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/765194>; Avelasco@hackingteam.it. "Meetings in Argentina". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/611846>; M.luppi@hackingteam.it. "Meetings in Argentina". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/600077>; Aскарfile@hackingteam.it. "Argentina-Hilton Demonstrations Schedule". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/593799>; M.bettini@hackingteam.it. "Resoconto Argentina". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/805712>; Avelasco@hackingteam.it. "Report on Argentina visit with final agenda attached". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/596983>

111 Fuentes del Ministerio Público Fiscal consultadas para este informe afirmaron que su dependencia no llegó a comprar el software de Hacking Team.

112 Ivan.sanchez@nullcode.com.ar. "Product Remote Control System". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/4135>; M.russo@wiseplant.com. "Product Remote Control System". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/4526>; M.russo@wiseplant.com. "Product Remote Control System". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/138576>

antes de concretar una visita a la Argentina, necesitaba más precisiones sobre las agencias a las que podía ofrecer su *software*. “El Gobierno nacional es un poco genérico. Cuando decimos usuario final nos referimos a la agencia que esté autorizada a investigar y esté interesada en nuestro producto. En cada país hay diferentes grupos que corresponden a policía, inteligencia, defensa, etc: cada uno es una agencia de y puede ser un usuario final, y necesitamos saber a quién quiere presentar su solución”.¹¹³

En segundo lugar, Tecnología Avanzada en Medidas y Contramedidas Electrónicas (TAM-CE) en 2014 y sobre todo en 2015, cuando el CEO Nicolás Ruggiero contacta a Hacking Team con la aspiración de celebrar reuniones con diversos organismos de inteligencia y defensa argentinos, como Gendarmería o la recién creada Agencia Federal de Inteligencia (AFI).¹¹⁴ Según los mails revelados por Wikileaks, Nicolás Ruggero se ofreció como intermediario para “mover influencias” y lograr que la AFI comprara los productos de Hacking Team. En un mail del representante de TAMCE hacia la empresa italiana se lee:

Estimados Philippe y Marco. Espero se encuentren bien. Les escribo para informarles que en el día de ayer, 23 de Junio, tuve la reunión con el Director de la AFI en nuestras oficinas y le hice una presentación y entregue la carpeta de HT. Les comente la seriedad de la empresa, donde está ubicada, que tienen 60 clientes activos alrededor del mundo y por sobre todo que es una empresa de capitales Italianos “independiente” del gobierno. También les mencione que cuentan con apoyo de personal técnico en idioma español de México y Colombia. Me informaron, que hace poco tiempo, que estuvieron en Buenos Aires unas personas de Israel de NSO Group, realizando la presentación de su solución PEGASO pero que aun NO CERRARON con nadie y siguen buscando soluciones. En estos días me estarán brindando una respuesta en relación a la presentación de HT en Buenos Aires Argentina, pero desde ya que los note muy interesado en el tema y si estoy seguro que van a comprar a corto plazo (ojala sea a nosotros).¹¹⁵

Según otro de los mails del intercambio, Ruggero intermediaba en favor de Hacking Team en la Argentina para que la agencia de inteligencia le comprara a ellos (y no a otra empresa israelí) el *software* de interceptación. Ante esta intermediación, el representante italiano respondía, el 25 de junio de 2015:

Hola Nicolas, Gracias por el update. Me parece muy bien que estamos a tiempo con AFI y que están buscando una solución ofensiva de intercep-

¹¹³ Idem.

¹¹⁴ “Argentina involucrada en el affair Hacking Team”. Segu Info-Información de Seguridad. 11 de julio de 2015. Consultado el 19 de octubre de 2015 <http://blog.segu-info.com.ar/2015/07/argentina-involucrada-en-el-affaire.html> y Adam Dubove. “Hacking Team hizo contactos en Argentina para vender software espía”. Panam Post. 13 de julio de 2015. Consultado el 19 de agosto de 2015. <http://es.panampost.com/adam-dubove/2015/07/13/hacking-team-hizo-contactos-en-argentina-para-vender-software-espia/>

¹¹⁵ Pvinci@hackingteam.com. “Re: NICOLAS>>(Tamce) Meeting”. E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/1088185>

ción. Tenemos muchos argumentos y diferenciadores en comparación con la solución de NSO (nos prepararemos a esto) y estoy seguro de que haremos una excelente presentación en la demo. Saludos Philippe.

Tercero, Global Interactive Group (GIG), quienes en abril de 2015 contactaron a Hacking Team, a través de su representante Alex Lawson, para intermediar y vender servicios al Ejército, Gendarmería, la Prefectura, la Policía Federal, la policía de las provincias y la AFI.¹¹⁶

Al igual que Ruggero, Alex Lawson de GIG también se ofreció como un intermediario para que Hacking Team llegara a la nueva agencia de inteligencia AFI y al Ejército, según consigna uno de los mails revelados.¹¹⁷

Si bien la compra del *software* de Hacking Team no se concretó, existen pruebas de que similares programas de espionaje fueron utilizados contra Alberto Nisman, el fiscal que investigaba el atentado terrorista contra la sede de la entidad judía AMIA (en 1994) y que murió en enero de 2015,¹¹⁸ poco antes de presentar una acusación contra la entonces Presidenta Cristina Kirchner por encubrimiento del atentado.

Consultados para este informe, representantes del Ministerio Público argentino señalan que, más allá de Hacking Team, existen otras empresas (grandes y pequeñas) que se acercan de forma periódica a jueces y fiscales para ofrecer servicios de interceptación de comunicaciones. También aclaran que es importante diferenciar comunicaciones y datos cifrados, siendo las comunicaciones un objetivo más fácil de interceptar, ya que en el caso de los datos, la Argentina cuenta con un problema previo que suele limitar la captación de comunicaciones: una red de telefonía celular

116 Alex.lawson@globalinteractivegroup.com. "RE: Att. Eduardo Pardo y Massimiliano Luppi Rtt. Alex Lawson". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/433276>; Alex.lawson@globalinteractivegroup.com. "RE: Att. Eduardo Pardo y Massimiliano Luppi Rtt. Alex Lawson". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/433277>; M.luppi@hackingteam.com. "RE: Att. Eduardo Pardo y Massimiliano Luppi Rtt. Alex Lawson". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/434521>; G.russo@hackingteam.com "Re: (Global Interactive Group) NDA & Partner PolicyE-mail". 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/407300>

117 "Estimados Eduardo y Massimiliano. Por la presente les solicito nos envíen el NDA para firmarlo y re enviárselos. También consultarles si disponen de los PDF en Español así como alguna información más disponible. Leí los documentos de la carpeta y los encontré excepcionalmente interesantes. Creo que tenemos un excelente mercado para vuestros productos en Argentina, solo se trataría de replicar la misma estructura de presentaciones que concretamos en Buenos Aires el año pasado a todas las fuerzas y organismos estatales con competencia, cuando presentamos los productos de Omnisec y Kudelski Security de Suiza. Se trataría de Ejército, Gendarmería, Prefectura, Policía Federal, Policía de las Provincias y AFI. Tenemos llegada a todas ellas. Saludos, Alex Lawson. CEO. Global Interactive Group SRL" M.luppi@hackingteam.com. "Opportunity Argentina" 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/4517>

118 Redacción. "La muerte de Alberto Nisman". Curaduría La Nación. Enero 2015. Consultado el 14 de febrero de 2016. <http://www.lanacion.com.ar/la-muerte-de-alberto-nisman-t53089>; Raúl Kollman. "A un año de la muerte de Nisman: Una trama de operaciones políticas y judiciales". 17 de enero de 2016. Consultado el 20 de enero de 2016. <http://www.pagina12.com.ar/diario/elpais/1-290509-2016-01-17.html>

deficiente, con cortes permanentes y una de las peores coberturas 4G del mundo.¹¹⁹

Por lo tanto, las comunicaciones a interceptar suelen ser las enviadas a través de redes de internet o *Wi-Fi*, pero menos efectivas cuando se realizan por redes de datos. En Argentina, el espionaje sobre equipos mediante programas de computación como el que vende Hacking Team no es legal porque no está expresamente regulado, aunque existen disposiciones específicas para la interceptación de comunicaciones privadas.

Interceptación de comunicaciones en un proceso penal

El artículo 18 de la Constitución de este país establece la inviolabilidad del domicilio y las comunicaciones privadas. El artículo 19 establece el ámbito de privacidad de las personas al decir que las acciones que estas realicen y que no “ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están (...) exentas de la autoridad de los magistrados”. Esto se lee para decir que se necesita un acto de algún magistrado para poder interceptar el ámbito privado de los argentinos.

La Ley de Argentina Digital remarcaba este derecho en su artículo 5º, al decir que son inviolables “la correspondencia, entendida como toda comunicación que se efectúe por medio de tecnologías de la información y las comunicaciones, entre las que se incluyen los tradicionales correos postales, el correo electrónico o cualquier otro mecanismo que induzca al usuario a presumir la privacidad del mismo y de los datos de tráfico asociados a ellos”. Su interceptación, así como su posterior registro y análisis, sólo procederá a requerimiento del juez competente.

Sin embargo, a pocos días de su asunción en diciembre de 2015, el presidente Mauricio Macri anuló, vía decreto de necesidad y urgencia, la Ley Argentina Digital y creó un nuevo Ministerio de Comunicaciones que tendrá, entre otras, la misión de presentar una nueva ley al Congreso. Por lo tanto, este artículo se encuentra en puertas de una discusión legislativa (de la legalidad o no del decreto) o de su modificación.¹²⁰

En esta misma línea, el artículo 16 del Código Procesal Penal de la Nación establece que para restringir o limitar el goce de derechos reconocidos por la Constitución o los instrumentos internacionales de derechos, se deben aplicar los principios de idoneidad, razonabilidad, proporcionalidad y necesidad. Si tomamos como presupuesto que el programa de RCS afecta el derecho a la privacidad y la inviolabilidad de las comunicaciones, y de manera indirecta el derecho a la libertad de expresión, estos principios deben necesariamente ser tomados en cuenta.

En cuanto a la interceptación de comunicaciones en sentido estricto, el artículo 143 del Código Procesal Penal de la Nación prevé que si resulta útil para la comprobación del

119 “Argentina, entre los países con peor cobertura 4G”. Infobae. 24 de septiembre de 2015. Consultado el 25 de enero de 2016. <http://www.infobae.com/2015/09/24/1757614-argentina-los-paises-peor-cobertura-4g>

120 Para más detalles y análisis al respecto, ver Martín Becerra. “Restauración”. QUIPI- Políticas y Tecnologías de Comunicación. 14 de enero de 2016. Consultado el 18 de febrero de 2016. <https://martinbecerra.wordpress.com/2016/01/14/restauracion/>

delito, el juez podrá ordenar, a petición de parte, la interceptación y secuestro de correspondencia postal, telegráfica, electrónica o cualquier otra forma de comunicación. Esta tiene carácter excepcional y solo podrá efectuarse por un plazo máximo de treinta días renovables. Asimismo establece una obligación para las empresas que brinden el servicio de comunicación de “posibilitar el cumplimiento inmediato” de esta diligencia, de otra forma podrían incurrir en responsabilidades penales.

De nuevo, el problema con el programa de RCS es que, en primer lugar, va mucho más allá de la mera interceptación de comunicaciones privadas. En segundo, y hasta donde sabemos, no tiene un límite temporal establecido. Y en tercer lugar, si bien la ley argentina se dirige a las empresas que brinden un servicio de comunicación, el *software* de Hacking Team interviene directamente las computadoras y celulares de las personas afectadas, por lo que no es exactamente equivalente.

Incautación de objetos y equipos

Una regla que está pensada para el mundo análogo pero que puede aplicarse a este caso por analogía, es la que se refiere a la incautación de equipos contemplada en el artículo 90 del Código Procesal Penal. Dice que en el marco de una investigación penal la policía debe “d) incautar los documentos y todo elemento material que pueda servir a la investigación, cuando les esté permitido” y “j) Reunir toda la información de urgencia que pueda ser útil al representante del Ministerio Público Fiscal”.

Si bien este artículo habla de “incautaciones” físicas, se puede hacer un paralelo para justificar la obtención y retención de información a partir del *software* de Hacking Team. En el caso argentino, es bastante problemático por ser la norma demasiado amplia y no establecer salvaguardas o garantías con respecto a la persona que está siendo investigada. Es decir, le da permiso a la policía de tomar prácticamente todo, sin controles judiciales previos o posteriores y sin discriminar entre pertenencias estrictamente privadas y aquellas que podrían tener relación con el juicio en cuestión.

Registro de sistemas informáticos

En la misma línea, el artículo 144 del Código Procesal Penal de la Nación establece que el juez puede ordenar el registro de un sistema informático o de un medio de almacenamiento de datos electrónicos para “obtener copia o preservar datos o elementos de interés”. Este tipo de registro sin duda está dentro de las capacidades del programa de espionaje de Hacking Team. La única diferencia es que, si bien el artículo se refiere a registros físicos, RCS puede hacer estas diligencias de forma remota y mediante la instalación subrepticia del *software*.

Por otro lado, el artículo 129 del mismo Código acota un poco las reglas, estableciendo que “no se podrán inspeccionar lugares y cosas, salvo que existiera motivo suficiente y fundado para presumir que se encontrarán elementos útiles para la investigación”. Dicha inspección se realiza por fuerzas de seguridad y puede estar presente un representante del Ministerio Público. Para que sea válida, dos testigos que no pertenezcan a la policía deben firmar un

acta. Este último requisito de validez es poco probable en el caso del *software* de RCS.

Como regla general –según el artículo 127 del Código Procesal Penal de la Nación– pueden probarse los hechos del caso por cualquier medio, salvo que se encuentren expresamente prohibidos por la ley y siempre que no vulneren derechos humanos. En este sentido, si se interviene una comunicación o se incauta un equipo sin orden judicial, las pruebas que se encuentren no podrían ser aceptadas en un juicio.

Intercepción de comunicaciones por agencias de inteligencia

La Ley de Inteligencia Nacional define las actividades de inteligencia nacional en su artículo 2 como aquellas “consistentes en la obtención, reunión, sistematización y análisis de la información específica referida a los hechos, amenazas, riesgos y conflictos que afecten la seguridad exterior e interior de la Nación”. También contempla otras definiciones como inteligencia criminal, contrainteligencia e inteligencia estratégica militar.

Tanto la Agencia Federal de Inteligencia como la Dirección Nacional de Inteligencia Criminal manifestaron su interés por comprar el *software* de RCS (aunque luego no lo hicieron). Sin embargo, la Ley de Inteligencia Nacional prohíbe que los organismos de inteligencia cumplan con funciones policiales o de investigación criminal, salvo si existe un requerimiento específico y fundado de un juez, en el marco de una investigación, o estén expresamente facultados por la ley. Tampoco pueden obtener información, producir inteligencia o almacenar datos sobre personas en base a criterios de raza, fe religiosa, acciones privadas, opinión política o de adhesión o pertenencia a organizaciones partidarias, sociales o sindicales, ni en función de cualquier otra actividad legal que realicen.

En este sentido, según la Asociación por los Derechos Civiles (ADC), para la intercepción de las comunicaciones hay un único organismo facultado: el Departamento de Intercepción y Captación de las Comunicaciones (D.I.COM), dependiente de la Dirección General de Investigaciones y Apoyo Tecnológico a la Investigación Penal (D.A.T.I.P.), perteneciente a su vez a la estructura del Ministerio Público Fiscal de la Nación.¹²¹ El fundamento de esta afirmación es el artículo 17 de la Ley 27.126.¹²²

El D.I.COM fue establecido en julio de 2015, bajo la órbita de la Procuración General de la Nación y ocupó un viejo edificio de la antigua Secretaría de Inteligencia del Estado (SIDE), que funcionó en Argentina desde 1946 hasta 2015. Desde su inicio, la oficina se encargó de profesionalizar y transparentar los procesos de intercepción de comunicaciones y establecer un protocolo de actuación.¹²³ Al cierre de este informe, sin embargo, el nuevo Gobierno argentino de Mauricio Macri había transferido, vía decreto de necesidad y ur-

121 Asociación por los Derechos Civiles. “Educar para Vigilar”. Diciembre de 2015. Consultado el 4 de enero de 2015.
<https://adcdigital.org.ar/2016/01/29/educar-para-vigilar/>

122 Ídem.

123 Irina Hauser. “No sólo un cambio de manos”. Página 12. 7 de julio de 2015. Consultado el 4 de agosto de 2015.
<http://www.pagina12.com.ar/diario/elpais/1-276542-2015-07-07.html>

gencia, las escuchas telefónicas a la órbita de la Corte Suprema.¹²⁴ La respuesta del máximo organismo judicial del país fue que no contaba con “los medios humanos y materiales” necesarios para realizar dicha tarea y que postergaba la decisión hasta el 15 de febrero. “No es posible llevar adelante de inmediato esa misión, dada su especificidad, en tanto involucra la organización de medios humanos y materiales, así como una prolija tarea reglamentaria”, señalaron sus autoridades.¹²⁵

De cualquier forma, el artículo 5° de la Ley de Inteligencia Nacional es muy claro al decir que cualquier tipo de comunicación o información, archivos, registros o documentos “son inviolables en todo el ámbito de la República Argentina, excepto cuando mediare orden o dispensa judicial en sentido contrario”. Es decir que en todo caso, inclusive la D.I.COM necesitaría de una orden judicial.

A pesar de la claridad de esta disposición, la Asociación por los Derechos Civiles resalta que “coexisten múltiples organizaciones o unidades de inteligencia en las distintas fuerzas armadas y de seguridad, tanto federales como provinciales, como así también organismos encargados de investigaciones criminales que pueden tener acceso a este tipo de tecnologías”.¹²⁶

Sanciones

La misma Ley de Inteligencia Nacional, en su artículo 42, castiga con tres a diez años de cárcel a quien indebidamente intercepte, capte o desvíe comunicaciones telefónicas, postales o de cualquier otro sistema de “transmisión de imágenes, voces, paquetes de datos” o documentos privados.

5.2. Guatemala

En este país, Hacking Team se reunió con la Dirección de Análisis Criminal de Guatemala, una dependencia adscrita al Ministerio Público, que buscaba capacitar a 200 agentes para que pudieran utilizar el *software* de espionaje.¹²⁷ El Gobierno de Guatemala argumentó que esta dirección era la única con facultades para realizar las actividades e intromisiones que provee RCS.

Al igual que en Honduras, la compañía intermediaria fue NICE Systems, representada por Ori Zoller, un ex militar israelí dedicado a la venta de armas AK-47 que eventualmente terminaron en manos de grupos paramilitares de Colombia.¹²⁸ Las negociaciones se pactaron por un precio de 450

¹²⁴ Redacción. “Macri transfirió las escuchas telefónicas a la Corte Suprema con un DNU”. Telam. 29 de diciembre de 2012. Consultado el 14 de enero de 2016. <http://www.telam.com.ar/notas/201512/131473-escuchas-corte-dnu.html>

¹²⁵ Redacción. “La Corte postergó la aplicación de otro ‘decreto de necesidad y urgencia’ de Macri”. Página 12. 29 de diciembre de 2015. Consultado el 14 de enero de 2016. <http://www.pagina12.com.ar/diario/ultimas/20-289216-2015-12-29.html>

¹²⁶ Ibidem, Asociación por los Derechos Civiles.

¹²⁷ Dvincenzetti@hackingteam.com. “FWD: Guatemala”. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/173519>

¹²⁸ Lee Fang. “Former AK-47 Dealer Goes Cyber, Supplied Surveillance Tools to Honduras Government”. The

mil euros¹²⁹ y existía incluso una fecha de entrega a finales del año 2013, pero la misma nunca se concretó porque el Gobierno guatemalteco no pudo autorizar el pago.¹³⁰

En enero de 2014, Aristeo Sánchez de la Unidad de Métodos Especiales del Ministerio Público, escribió a Hacking Team esperando retomar las negociaciones para incluir el programa Galileo en el Plan Anual de Operaciones del país.¹³¹ A finales de febrero de ese mismo año, Ori Zoller envió un correo a Massimiliano Luppi, el administrador de las cuentas de Hacking Team, diciéndole que estaban a dos semanas de cerrar el trato con Guatemala y obtener el primer pago.¹³² No hubo intercambio de correos posteriores sobre el tema.

Como regla general, el artículo 24 de la Constitución establece que la correspondencia, documentos y libros de una persona son inviolables y solo pueden revisarse o incautarse si existe una resolución judicial. Se garantiza también el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas y de “otros productos de la tecnología moderna” que pueden incluir los programas y aplicaciones a los que Galileo tiene acceso.

También establece que “los documentos o informaciones obtenidas con violación de este artículo no producen fe ni hacen prueba en juicio”. Es decir, como regla general, si se obtiene información con métodos intrusivos como los que vende Hacking Team, y no se tiene una orden judicial para justificar su uso, las pruebas obtenidas serían inválidas. El artículo 183 del Código Procesal Penal confirma cuando dice que son inadmisibles los elementos de prueba obtenidos por un medio prohibido como es la “indebida intromisión” en la intimidad del domicilio, la correspondencia, las comunicaciones, los papeles y los archivos privados.

Interceptación de comunicaciones en procesos penales

Esta actividad se regula en los artículos 203 a 205 del Código Procesal Penal. La regla general se refiere al secuestro de correspondencia “cuando sea de utilidad para la averiguación” y debe estar fundamentada en una orden del juez que esté a cargo del procedimiento o del presidente del Tribunal Colegiado en su caso. Si es un caso de flagrancia, el Ministerio Público podrá expedir la orden, pero el tribunal o el juez tienen que ratificarla.

Intercept. 27 de julio 2015. 9 de marzo de 2016. <https://theintercept.com/2015/07/27/ak-47-arms-dealer-goes-cyber-supplied-surveillance-tools-honduras-government/> y M.luppi@hackingteam.com. “R: Guatemala”. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/446530>

129 M.bettini@hackingteam.it. “Re: Plan Q1”. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/3195>

130 D.milan@hackingteam.com. “Fwd: Guatemala delivery”. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/517846>; G.russo@hackingteam.com. “Fwd: Re: hardware requirements”. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/446475>; M.luppi@hackingteam.com. “I: Guatemala payment”. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/455941>

131 Aristeosanchez@gmail.com. “Re: Propuesta”. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/249820>

132 M.luppi@hackingteam.com. “Update Guatemala”. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/5071>

El Código Procesal Penal reglamenta qué hacer una vez que se recibe la correspondencia por los tribunales. El juez lee cada elemento incautado y si tienen relación con el procedimiento, ordena su secuestro. Si no tienen relación, se debe regresar al dueño o a un pariente cercano. Sin embargo, este supuesto no podría ser aplicable al *software* de espionaje de Hacking Team, pues al tener control sobre la computadora o teléfono celular de la persona inoculada, todo el contenido es legible y de todo se puede guardar una copia, sin importar la relación de la información con el proceso penal en turno.

Estas mismas reglas aplican al “control y grabación de comunicaciones telefónicas o similares”. Su resultado y grabación solo podrán ser entregados al tribunal que los ordenó y se deben destruir las grabaciones que no tengan relación con el procedimiento. Por último, también se establece que la persona que intercepte o grabe la comunicación tiene la obligación de guardar secreto sobre su contenido, salvo que se le cite como testigo en el procedimiento. Las reglas no parecen aplicables a la interceptación de equipos completos, como lo facilita RCS.

Incautación e inspección de objetos

El Código Procesal Penal establece las reglas de inspección y registro de objetos en su artículo 187 cuando fuera necesario “porque existen motivos suficientes para sospechar que se encontrarán vestigios del delito”. Además “se recogerán o conservarán los elementos probatorios útiles”. En todo caso, el control también es estricto pues se debe levantar un acta que describa exactamente lo que pasó. En esta misma línea, el artículo 198 establece que las cosas y documentos relacionados con el delito o que pudieran ser de importancia para la investigación y los sujetos a comiso serán depositados y conservados del mejor modo posible.

El artículo 199 establece que hay ciertas cosas que no se pueden secuestrar, como las comunicaciones escritas entre el imputado y las personas que puedan abstenerse de declarar como testigos por razón de parentesco o secreto profesional y las notas que estos hubieran tomado sobre comunicaciones confiadas por la persona procesada.

Estas limitaciones son importantes si pensamos en el *software* de espionaje de Hacking Team, pues por sus capacidades técnicas, es sumamente difícil hacerlas valer. Las reglas de incautación, en este caso, tampoco parecen aplicables, por tratarse de una inspección física.

Interceptación de comunicaciones por agencias de inteligencia

La Ley Contra la Delincuencia Organizada establece que para evitar, interrumpir o investigar la comisión de delitos regulados en misma ley, podrán interceptarse, grabarse y reproducirse todo tipo de comunicaciones, siempre y cuando medie una autorización judicial.¹³³

Con base en este ordenamiento, la Comisión Internacional Contra la Corrupción en Guatemala implementó el Acuerdo Interinstitucional para Establecer e Implementar el Sistema

¹³³ Katitza Rodríguez, Marlon Hernández Anzora, Hedme Sierra-Castro, Jorge Jiménez Barillas, Edy Tábora Gonzales, y Mireya Zepeda Rivera. “¿Privacidad digital para defensores y defensoras de derechos humanos?”. 146. Consultado el 19 de enero de 2016. <http://acceso.or.cr/files/Investigacion-Privacidad-Digital-FA.pdf>

de Interceptación de Comunicaciones. Este crea el Centro de Monitoreo de Comunicaciones –ejecutado por agentes de la Policía Nacional Civil– para interceptar comunicaciones telefónicas y geolocalizar. El Ministerio Público lo ejecuta, previa autorización judicial. La Dirección de Análisis Criminal –el organismo que negoció con Hacking Team– tiene facultades para solicitar la interceptación de llamadas en tanto es un organismo adscrito al Ministerio Público, pues se dedica a recabar información criminal y la analiza para convertirla en insumos útiles para la persecución penal.¹³⁴

A su vez, la Ley Marco del Sistema Nacional de Seguridad limita el alcance del espionaje por agencias de inteligencia. En el artículo 21 se define el “Ámbito de Inteligencia del Estado”, que se refiere a la articulación de “información e inteligencia de amenazas, riesgos y vulnerabilidad internas y externas”. Actúa bajo la responsabilidad del Presidente de la República, por conducto del Secretario de Inteligencia Estratégica del Estado.

En este sentido, según el artículo 24, los facultados para producir inteligencia y conducir actividades de contrainteligencia son la Secretaría de Inteligencia Estratégica de Estado, la Dirección de Inteligencia Civil del Ministerio de Gobernación y la Dirección de Inteligencia del Estado Mayor de la Defensa Nacional del Ministerio de la Defensa Nacional. Sin embargo, no existen facultades específicas para la interceptación de comunicaciones. En cualquier caso, en los artículos 25 a 29 se amplía el concepto de “inteligencia” para que pueda desprenderse esta actividad de estas prácticas. Algo tan intrusivo como el propio *software* de Hacking Team debería tener una regulación muy específica, inclusive cuando su uso es por parte de agencias de inteligencia.

Aún así, el Sistema de Guatemala tiene establecidos mecanismos de contrapeso para garantizar la imparcialidad en la fiscalización de las actuaciones del Sistema Nacional de Seguridad y de las instituciones que lo integran, por parte de los organismos judiciales y legislativos en el artículo 32 de la ley.

La Ley de la Dirección General de Inteligencia Civil (DIGICI) permite limitaciones al derecho a la privacidad en su artículo, 4 en los casos que existan indicios de actividades del crimen organizado en las que peligre la vida, la integridad física, la libertad y los bienes de personas determinadas. El Ministerio Público puede, en este contexto, solicitar de manera urgente la autorización de una Sala de la Corte de Apelaciones para interceptar comunicaciones de manera temporal. Los estándares de la Ley de Delincuencia organizada se mantienen.¹³⁵ En todo caso, el *software* de Hacking Team no se acoge a estas disposiciones, porque va mucho más allá de la interceptación de comunicaciones y es más invasivo.

134 “Conversando con la Fiscal General y Jefa del MP”. Industria Guatemala. CICG. Consultado el 18 de noviembre de 2015. <http://industriaguatemala.com/conversando-fiscal-general-jefa-del-mp>

135 Ibidem. Fundación Acceso, 148.

Sanciones

En su artículo 219, el Código Penal de Guatemala castiga con multa a quien, con medios fraudulentos, intercepte, copie o grabe comunicaciones de cualquier tipo. Esta misma actividad se sanciona con cárcel según el artículo 220 si a) el autor se aprovecha de su calidad de funcionario público b) si se tratare de asuntos oficiales o c) la información se hiciera pública, por cualquier medio.

5.3. Paraguay

En 2012, el Gobierno del ex presidente Federico Franco adquirió un equipo de escuchas telefónicas por US\$2,5 millones, que misteriosamente desapareció de las oficinas del Ministerio del Interior, según relató un informe de la Auditoría General del Poder Ejecutivo en noviembre de 2013.

Relativo a Hacking Team, la Unidad de Delitos Informáticos del Ministerio Público negoció la compra de *software* de espionaje a la compañía italiana por vía del intermediario de seguridad, Radar. La serie de correos filtrados se corta en mayo de 2014.¹³⁶ En octubre de 2014, el socio local de Hacking Team solicitó un equipo adicional, lo que evidencia que hubo un seguimiento de la oferta por parte de las autoridades paraguayas.¹³⁷

Según los correos, el Estado paraguayo estuvo interesado en adquirir Galileo para la persecución de hechos punibles con énfasis en terrorismo y narcotráfico, por el valor de 620 mil euros, más 65 mil euros por mantenimiento anual.¹³⁸ Sin embargo, la compra no fue concretada. El fiscal de delitos informáticos, Ariel Martínez, dijo a Radio Cardinal y luego a ABC Color que, a pesar del ofrecimiento que hubo, no se compró programa alguno para espiar a los ciudadanos.¹³⁹

Paraguay se expande tecnológicamente con sistemas avanzados de vigilancia de las comunicaciones, pero sin las salvaguardas adecuadas. No existen regulaciones que obliguen a una rendición de cuentas, a la supervisión pública con respecto al uso y alcance de los poderes y técnicas de vigilancia de las comunicaciones, ni de reportes de transparencia, tanto en el proceso penal y/o de inteligencia. Si bien la compra de Galileo no se concretó, el Estado paraguayo sí compró FinFisher, según la investigación de CitizenLab de la Universidad de Toronto.¹⁴⁰

136 http://www.abc.com.py/nacionales/estado-negocio-espionaje-1385872.html?utm_content=bufferdb42e&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

137 <https://wikileaks.org/hackingteam/emails/emailid/249367>

138 La fiscalía remarca su esfuerzo en perseguir a la guerrilla del Ejército del Pueblo Paraguayo (EPP), supuesta agrupación terrorista en el territorio paraguayo. Ver https://es.wikipedia.org/wiki/Ej%C3%A9rcito_del_Pueblo_Paraguay

139 http://www.cardinal.com.py/noticias/fiscal_ariel_martnez_nunca_consideramos_la_compra_de_equipos_de_espionaje_nos_ofrecieron_siempre_pero_nunca_compramos_33440.html y <http://www.abc.com.py/nacionales/estado-negocio-espionaje-1385872.html>

140 Bill Marczak, John Scott-Railton, Adam Senft, Irene Poetranto, and Sarah McKune, "Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation", CitizenLab. 15 de Octubre de 2015.

Tampoco se cuenta con una supervisión por parte de un órgano independiente que autorice la solicitud de vigilancia. No existen mecanismos de notificación al usuario afectado en el proceso penal ni de inteligencia, con el objeto de que la ciudadanía pueda ejercer un control democrático de las autoridades.

Como regla general, la Constitución de Paraguay establece en su artículo 36 que todo el patrimonio documental de las personas es inviolable. Es decir, que los registros, impresos, correspondencias, escritos o cualquier especie de comunicación “no podrán ser examinados, reproducidos, interceptados o secuestrados sino por orden judicial” y siempre que fuesen indispensables para aclarar algún asunto confrontándose al derecho de la privacidad e intimidad mencionado en la Constitución en su artículo 33.

Es decir que si con el *software* de Hacking Team se obtiene información sin contar con el respaldo de una orden judicial, estas mismas no podrían ser utilizadas como prueba en un juicio. El artículo 174 del Código Procesal Penal refuerza esta idea, estableciendo que los actos que vulneren derechos humanos no son válidos como prueba.

Interceptación de comunicaciones privadas en procesos penales

El artículo 198 del Código Procesal Penal regula la interceptación y secuestro de correspondencia siempre que sea útil para la investigación y sea ordenada por el juez. Por otro lado, los artículos 198, 199, 200 y 228 de este mismo Código regulan reglas básicas para proceder a la interceptación de las comunicaciones.

Los elementos de prueba solo pueden ser valorados si han sido obtenidos por medios legales. Específicamente se deben cumplir los siguientes requisitos: a) orden judicial (la falta de dicha autorización es causal de nulidad del procedimiento) b) que únicamente el juez de la causa tiene la potestad de ordenar la interceptación c) que el juez es quien se encarga del contenido de la información interceptada, poniéndola a conocimiento del Ministerio Público, debiendo destruir la evidencia a *posteriori* y d) la interceptación tiene carácter de excepcionalidad.

Sin embargo, el artículo 200 de este Código Procesal Penal otorga al Juez la potestad de elegir “cualquiera sea el medio técnico utilizado para conocer” la comunicación del imputado. Este apartado abre la posibilidad a una laguna legal para las interpretaciones sobre el uso de herramientas inclusive de carácter malicioso, una forma de vigilancia considerada más invasiva que una mera interceptación de comunicaciones. Cabe preguntarse si los organismos que pretendían la adquisición de *software* de Hacking Team tenían esta disposición en mente para el despliegue de las capacidades intrusivas de RCS.

Incautación de objetos

En cuanto al secuestro de objetos, los artículos 193 a 198 del Código Procesal Penal establecen la regulación y los límites del mismo. No se pueden secuestrar a) las comunicaciones escritas entre el imputado y las personas que puedan abstenerse de declarar como

Disponible en: <https://citizenlab.org/2015/10/mapping-finfofishers-continuing-proliferation/>

testigos b) las comunicaciones entre el imputado y su abogado c) los resultados de exámenes o diagnósticos relativos a las ciencias médicas realizados bajo secreto profesional. El artículo 195 continúa diciendo que la orden de secuestro será expedida por el juez, en una resolución fundada.

Es dudoso que estas reglas sean aplicables a la inspección a distancia, como es posible a través de RCS. Como mínimo, el *software* de espionaje de la empresa Hacking Team debería respetar estos parámetros, aunque por sus mismas capacidades técnicas y alto grado de interceptación, el respeto a las comunicaciones inviolables es difícil de monitorear.

Interceptación de comunicaciones por agencias de inteligencia

Por otro lado, en cuanto al espionaje por parte de agencias de inteligencia, la Ley N° 5241/2014 que crea el Sistema Nacional de Inteligencia otorga a este último competencias plenas a nivel nacional en materia de inteligencia y contrainteligencia. Esta entidad tiene la autoridad para “recopilar y procesar” información con el objetivo de producir inteligencia y tiene muchas facultades para interceptar comunicaciones. Se debe contar con autorización judicial previa, bajo pena de nulidad, excepcionalidad e indispensabilidad de interceptación de las comunicaciones en cualquiera de sus formas. Además, solo puede hacerse cuando la interceptación tiene relación con bienes jurídicos o intereses establecidos en la norma. Por último, debe hacerse por un tiempo limitado y se deben identificar de forma muy precisa las personas a ser investigadas.¹⁴¹

Otra institución vinculada a la vigilancia estatal fuera del ámbito penal es la Secretaría Nacional Antidrogas (SENAD), institución que tiene bajo su órbita el combate al tráfico de drogas y estupefacientes. Tiene la potestad de interceptar excepcionalmente las comunicaciones y correspondencias en todas sus formas, previa autorización de un juez competente bajo pena de nulidad, con limitaciones en el tiempo de la interceptación.¹⁴²

Lo preocupante es que no queda claro cuáles son las áreas y los límites de investigación de la Agencia de Inteligencia. Por tanto, da pie a que sistemas como Hacking Team o cualquier *software* malicioso pueda ser utilizados desproporcionadamente por la agencia de inteligencia e instituciones vinculadas a la vigilancia estatal, aun cuando el control remoto de equipos parece ir mucho más allá de las facultades de interceptación de comunicaciones.

Sanciones

Como último punto, si alguna persona –incluyendo a funcionarios públicos– llegara a utilizar el *software* de Hacking Team sin consentimiento de la persona infectada, o sin orden judicial para tal efecto, el artículo 146 del Código Penal de Paraguay los sanciona con cárcel de uno a cuatro años si “lograra mediante medios técnicos, sin apertura del cierre, conocimiento del contenido de tal publicación para sí o para un tercero”. Además también existe el delito de acceso indebido a datos del artículo 146b de este mismo Código, mismo

¹⁴¹ Artículo 6, 24, 25, 26 y 27 de la Ley N.º 5241/14

¹⁴² Ley 1881/88 que modifica la Ley 1340. “Que Reprime el Tráfico Ilícito de Estupefaciente y drogas peligrosas y otros delitos afines y establece medidas de prevención y recuperación de farmacodependientes”. Artículos 88, 89, 91.

que cubre una laguna de punibilidad del fenómeno denominado *hacking* y que afecta el ámbito de la inviolabilidad de la vida y la intimidad de un individuo. Dicho de una manera más sencilla, el acceso indebido de datos sería una versión electrónica de la violación de domicilio prevista en el art. 141 del Código Penal. Su tipificación igualmente se adapta a la recomendación del artículo 2 del Convenio de Budapest del 2001.

5.4. Uruguay

El 9 de mayo de 2014, el equipo de Hacking Team se reunió en Uruguay con el entonces coordinador de Inteligencia del Estado, Ramón Bonilla, y con el director Nacional de Policía, Julio Guarteche. Ambos funcionarios quedaron muy impresionados con el producto de la empresa¹⁴³ y se comprometieron a interceder ante José Mujica, entonces Presidente, para convencerlo de las ventajas de adquirir el nuevo programa de vigilancia.

El Gobierno ya había comprado en 2013 El Guardián, un avanzado sistema de espionaje brasileño que potencia la capacidad del Estado uruguayo para interceptar llamadas, correos electrónicos y redes sociales, además de sistematizar la información recolectada y ofrecer otras funciones.¹⁴⁴

En este país se regula la interceptación de comunicaciones estableciendo el requisito previo de orden judicial, pero el uso de *softwares* de espionaje como el de Hacking Team no está regulado y excede por mucho los mínimos legales.

Interceptación de comunicaciones en procesos judiciales

En términos generales, la Constitución establece en su artículo 28 que los papeles y todo tipo de correspondencia de los particulares son inviolables y nunca podrá hacerse su registro, examen o interceptación sino conforme a las leyes y por razones de interés general.¹⁴⁵

Las actividades de vigilancia de comunicaciones dentro de procesos judiciales se regulan en el Código del Proceso Penal. Este último establece en su artículo 146.2 que la vigilancia puede ser utilizada como un medio de prueba no prohibido por ley.

Según un reciente reporte publicado por Electronic Frontier Foundation, el procedimiento para que opere la vigilancia consiste en: a) la autorización de la vigilancia electrónica debe constar en resolución fundada del juez b) debe existir un memorándum

143 S.solis@hackingteam.it. "Paraguay-Uruguay Report". 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/455941>

144 Gonzalo Terra. "Gobierno de Mujica sondeó compra de más equipos de espionaje". El País Uruguay. 10 de julio de 2015. Consultado el 2 de febrero de 2016. http://www.elpais.com.uy/informacion/gobierno-mujica-sondeo-compra-mas.html?utm_content=buffer76b35&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

145 Fabrizio Scrollini, Ana Tudurí, y Katitza Rodríguez. "Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Uruguay". Electronic Frontier Foundation. Diciembre de 2015. Consultado el 15 de enero de 2016. <https://www.eff.org/es/country-reports/Uruguay-ES-final>

policial que establezca los motivos de la investigación que fundamentan la solicitud al fiscal c) el fiscal debe fundamentar por qué motivo la realiza.¹⁴⁶

Por otro lado, la Ley N° 18.494 sobre control y prevención de lavados de activos y del financiamiento del terrorismo, establece en su artículo 5 que la vigilancia electrónica es un medio al que puede recurrirse en la investigación de ciertos delitos.¹⁴⁷ Esta vigilancia abarca la interceptación telefónica, mensajes de texto, correos electrónicos, interceptación de teléfonos satelitales, cámaras de vídeo, micrófonos y metadatos,¹⁴⁸ por lo que cabe preguntarse si el *software* que Hacking Team vende puede caber aquí. El artículo establece que “quedan expresamente excluidas del objeto de estas medidas las comunicaciones de cualquier índole que mantenga el indagado con su defensor y las que versen sobre cuestiones que no tengan relación con el objeto de la investigación”. Por otro lado, al referirse a “todos los medios tecnológicos disponibles”, podría permitirse el uso de *malwares* como el de Hacking Team.

Incautación de objetos

Según el artículo 211, un juez puede disponer que aquellas cosas relacionadas con el delito que puedan servir como medios de prueba sean “conservadas o incautadas”. A su vez, el artículo 212 dice que si existen motivos graves para creer que la interceptación de la correspondencia o cualquier otra forma de comunicación en que el acusado esté involucrado puede ayudar a esclarecer el delito, el juez puede ordenarla y secuestrarla. Este último supuesto se refiere a comunicaciones telefónicas y no digitales, por lo que cabe preguntarse si podría aplicarle al caso del programa de RCS de Hacking Team.

Sin embargo, el artículo 214 establece un límite a estas actividades que difícilmente serían aplicables a los programas de espionaje de la empresa italiana: el que no pueden secuestrarse las cartas o documentos que se envíen o entreguen a los abogados de las personas acusadas.

Interceptación de comunicaciones por agencias de inteligencia

Por otro lado, en lo que concierne al espionaje o interceptación de comunicaciones por agencias de inteligencia, Uruguay tiene un proyecto de ley destinado a regular el llamado Sistema Nacional de Inteligencia.¹⁴⁹ El artículo 14 de este texto establece que “toda operación de búsqueda de información que deba realizar cualquier organismo componente del Sistema de Inteligencia del Estado, involucrando procedimientos especiales que puedan afectar la libertad y privacidad de los ciudadanos, deberá ser autorizada por el Poder Judicial”. El artículo 15 establece que hay ciertos principios que deben obedecerse como de legitimidad, eficiencia, financiamiento, legalidad, necesidad y diseminación.

Sanciones

Por último, el Código Penal uruguayo establece sanciones por el delito de violación de

¹⁴⁶ Ibidem, página 9.

¹⁴⁷ Ibidem, página 7.

¹⁴⁸ Idem.

¹⁴⁹ Ibidem, página 12.

correspondencia, en su artículo 296, a la persona que “con la intención de informarse de su contenido, abre un pliego epistolar, telefónico o telegráfico, cerrado, que no le estuviera destinado”. La pena es de multa y de uno a cuatro años de prisión. Es agravante del mismo si un funcionario público la comete.

El artículo 298 de este mismo ordenamiento establece que, si además estas comunicaciones se publican o comunican, se sanciona con multas adicionales.

5.5. Venezuela

Venezuela no figura como cliente en los archivos, sin embargo, el gobierno del ex presidente Hugo Chávez manifestó su interés para adquirir este tipo de *software*. Según un análisis de los correos filtrados, publicado por ArmandoInfo, el equipo de ventas de Hacking Team visitó tierras venezolanas la mañana del miércoles 6 de marzo de 2013, 24 horas después del anuncio de la muerte de Chávez.¹⁵⁰

Alex Velasco, el representante de ventas para América Latina, viajó a la capital venezolana con Alex Berroa y Richard Berroa de DTXT Corporation, una compañía de Estados Unidos dedicada a vender aplicaciones de seguridad que fungiría como intermediario en el proceso.

Previo a su llegada a Caracas, DTXT Corp envía un PDF donde especifica que “hay una instrucción presidencial” de recibirlos para mostrar la nueva solución de interceptación móvil, gracias al aumento de un 42% del uso de celulares en Venezuela en 2012.¹⁵¹ La idea era reunirse con el Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC), la División de Inteligencia Militar (DIM), la Dirección General de Contrainteligencia Militar (DGCIM) y la Dirección de Comunicaciones de la Fuerza Armada Nacional Bolivariana (DICOFANB).¹⁵²

El viernes de esa misma semana se reúnen con un general del Ejército venezolano y hacen una demostración en la que infectan en vivo un teléfono Android. El Primer Ministro no pudo llegar a la reunión debido a la muerte de Chávez.¹⁵³ Finalmente no se concretó ninguna compra.

Intercepción de comunicaciones en procesos penales

La Ley sobre Protección a las Comunicaciones Privadas establece en su artículo 6° que en el marco de un proceso judicial, las autoridades de policía podrán impedir, interrumpir, interceptar o grabar comunicaciones, únicamente a los fines de la investigación de los si-

150 Katherine Pennacchio. “Hacking Team casi Corona en Venezuela”. Armando Info. 18 de julio de 2015. Consultado el 19 de octubre de 2015. [http://www.armando.info/sitio/index.php?id=17&tx_ttnews\[tt_news\]=158&cHash=465c7aebd69ddc598ea041c78d4cf5ae](http://www.armando.info/sitio/index.php?id=17&tx_ttnews[tt_news]=158&cHash=465c7aebd69ddc598ea041c78d4cf5ae)

151 Idem.

152 Idem.

153 Idem.

guientes hechos: a) delitos contra la seguridad o independencia del estado b) delitos previstos en la Ley Orgánica de Salvaguarda del Patrimonio Público c) delitos contemplados en la Ley Orgánica sobre Sustancias Estupefacientes y Psicotrópicas y e) delitos de secuestro y extorsión.

En estos casos, se debe solicitar al juez penal para que autorice la interceptación, misma que no puede exceder de 60 días pudiendo prorrogarse. El juez debe notificar al Fiscal del Ministerio Público. Se establece también que, en casos de extrema urgencia, se puede interceptar sin orden judicial, siempre y cuando se notifique al juez penal (artículo 7). Toda grabación autorizada será de uso exclusivo de las autoridades policiales y judiciales encargadas de su investigación y procesamiento, por lo que queda prohibido divulgar la información (artículo 8).

Interceptación de comunicaciones por agencias de inteligencia

El artículo 5 de la Ley del Sistema Nacional de Inteligencia y Contrainteligencia define estas actividades como “los esfuerzos de búsqueda, producción, difusión de información, planificación y ejecución de operaciones concernientes a la seguridad, defensa y desarrollo integral” del país. En su mayoría, como lo dice el artículo 4, se concentran y subordinan al Ejecutivo Federal, es decir, el Presidente.

Por otro lado, el artículo 6 de esta ley establece que los organismos del Sistema Nacional de Inteligencia están facultados para “obtener, procesar y suministrar” al Presidente todo tipo de información de naturaleza estratégica en tiempo real y de carácter predictiva para garantizar la seguridad del país. El artículo 8 lo delimita un poco más, al decir que la actividad de inteligencia comprende “la planificación y ejecución de acciones tendientes a la obtención, procesamiento y difusión del conjunto de informaciones y documentos que se produzcan sobre las formas de actuación de personas” para detectar de manera preventiva las posibles amenazas al país. La definición es problemática pues, además de ser demasiado amplia, no permite explícitamente la interceptación de comunicaciones, mucho menos la interceptación de equipos y dispositivos enteros.

Existen al menos tres organismos cuyas competencias podrían incluir el uso de este tipo de *software*: el Servicio Bolivariano de Inteligencia, el Centro Estratégico de Seguridad y Protección a la Patria y la Comisión Nacional de Telecomunicaciones.

En cuanto al primero, la Gaceta Oficial N°39.436 establece que sus facultades son “contribuir con el sistema Nacional de Inteligencia y Contrainteligencia” y “desarrollar proyectos y tecnologías de la información que contribuyan a la obtención veraz y oportuna de información de interés para el alto gobierno”. No se le permite expresamente intervenir comunicaciones y sus facultades, si bien amplias, no son lo suficientemente claras para justificar una intrusión como la del *software* de Hacking Team.

La situación es similar en cuanto al segundo organismo, el Centro Estratégico de Seguridad y Protección a la Patria creado y regulado por el Decreto Presidencial N° 458, pues dentro de sus facultades está “suministrar información oportuna y de calidad que facilite

al Presidente de la República la toma de decisiones estratégicas y neutralizar potenciales amenazas a los intereses nacionales». Este suministro de información no implica la interceptación de equipos o comunicaciones privadas.

Por último, en cuanto a la Comisión Nacional de Telecomunicaciones, el artículo 37 establece que entre sus facultades está “requerir de los usuarios y de los operadores de servicios, las informaciones que considere convenientes” relacionadas con su materia. De nueva cuenta no faculta para intervenir comunicaciones privadas y mucho menos para interceptar equipos informáticos en su totalidad, como lo hace el *software* de Hacking Team.

Sanciones

La Ley sobre Protección a la Privacidad de las Comunicaciones en Venezuela establece en sus artículos 2º y 3º las penas de prisión a quien “arbitraria, clandestina o fraudulentamente grabe o se imponga de una comunicación entre otras personas, la interrumpa o impida” y a quien “sin estar autorizado, conforme a la presente Ley, instale aparatos o instrumentos con el fin de grabar o impedir las comunicaciones entre otras personas”.

6. Conclusiones generales

En América Latina las actividades de vigilancia y espionaje gubernamental resultan dignas de suspicacia, especialmente si tomamos en cuenta el historial de autoritarismos y represión en la región. Programas de espionaje tan invasivos como el de Hacking Team se prestan a abusos y violaciones de derechos humanos.

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, cuando se usan métodos como el *malware*, estos objetivos se logran mediante mecanismos secretos y posiblemente ilegales, con poca rendición pública disponible cuando precisamente, por el objetivo democrático que persiguen, deben ser objeto de controles ciudadanos y rendición de cuentas.

En general, las actividades de vigilancia y de recolección de información con fines de inteligencia está sujeta al respeto de estándares legales y constitucionales, como lo son los márgenes del debido proceso y el resguardo de derechos fundamentales, como la vida privada y la inviolabilidad de las comunicaciones. Por esta razón, medidas de investigación como la vigilancia de las comunicaciones privadas están normadas de forma especial. 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.¹⁵⁴

En el ámbito de la intervención de comunicaciones con fines de inteligencia, no solamente cabe asegurar resguardos sobre los mecanismos legales de recolección de información, sino que se deben delimitar conceptos como “seguridad nacional” y “orden público”. 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.¹⁵⁵

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

154 Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones.
<https://es.necessaryandproportionate.org/text>

155 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>

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 encargadas de la vigilancia de comunicaciones y correctamente capacitadas para ejercerlas.¹⁵⁶ 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.¹⁵⁷

Estos controles judiciales deben ser *ex ante* y autorizar las medidas invasivas, 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. 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 periodo y destrucción de la 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 esta o las que se realicen de manera clandestina deben ser sancionadas.¹⁵⁸ 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.

Cada juez y agencia de inteligencia, así como las instituciones de las que dependen, deben tener mecanismos claros de actuación dentro de 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.

¹⁵⁶ Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones <https://es.necessaryandproportionate.org/text>

¹⁵⁷ Idem.

¹⁵⁸ 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>

Bibliografía

- “Argentina involucrada en el affaire Hacking Team”. Segu Info-Información de Seguridad. 11 de julio de 2015. Consultado el 19 de octubre de 2015. <http://blog.segu-info.com.ar/2015/07/argentina-involucrada-en-el-affaire.html>
- “Argentina, entre los países con peor cobertura 4G”. Infobae. 24 de septiembre de 2015. Consultado el 25 de enero de 2016. <http://www.infobae.com/2015/09/24/1757614-argentina-los-paises-peor-cobertura-4g>
- “Briefing for the Italian Government on Hacking Team”. Privacy International. Abril y mayo de 2015. Consultado el 19 de septiembre de 2015. <https://privacyinternational.atavist.com/hackingteamsurveillanceexports>.
- “Conversando con la Fiscal General y Jefa del MP”. Industria Guatemala. CICG. Consultado el 18 de noviembre de 2015. <http://industriaguatemala.com/conversando-fiscal-general-jefa-del-mp>
- “Hacking Team Manifest”. Pastebin. 7 de julio de 2015. Consultado el 9 de marzo de 2016. <http://pastebin.com/TKK7BCSK>
- “Hacking Team, Chile y Ecuador”. People Tor Project. 11 de julio de 2015. Consultado el 16 de septiembre de 2015. https://people.torproject.org/~ilv/ht_chile_ecuador.html
- “La Empresa Hacking Team fue infiltrada y entre sus clients Panamá”. Algo Más Duro. 7 de Julio de 2015. Consultado el 14 de octubre de 2015. <http://www.algomasduro.com/inicio/tecnologia/39335-la-empresa-hacking-team-fue-infiltrada-y-entre-sus-clientes-panama>
- “Portal De Educação Do Exército Brasileiro”. Ensino. 2015. Consultado el 9 de marzo de 2016. <http://www.ensino.eb.br/exibeDetalhesCurso.do?curso=418>.
- “The Wassenaar Arrangement On Export Controls for Conventional Arms and Dual-Use Goods and Technologies”. The Wassenaar Arrangement Home Webpage. Consultado el 11 de enero de 2016. <http://www.wassenaar.org/>.
- Adam Dubove. “Hacking Team hizo contactos en Argentina para vender *software* espía”. Panam Post. 13 de julio de 2015. Consultado el 19 de agosto de 2015. <http://es.panam-post.com/adam-dubove/2015/07/13/hacking-team-hizo-contactos-en-argentina-para-vender-software-espia/>
- Agencia AFP. “Corte Suprema de Panamá ordena detención de expresidente Martinelli”. Diario El Telégrafo. 22 de diciembre de 2015. Consultado el 23 de diciembre de 2015. <http://www.eltelegrafo.com.ec/noticias/mundo/9/corte-suprema-de-panama-ordena-detencion-de-expresidente-martinelli>
- Andrés Delgado. “Cámaras en los moteles: “Solo vigilamos los pasillos”. 3 de marzo de

2015. Consultado el 10 de marzo de 2016. <http://andres.delgado.ec/2015/03/08/camaras-en-los-moteles-privacidad-ecuador-intimidad/>
- Arturo Angel. “México, el principal cliente de una empresa que vende software para espiar”. Animal Político. 7 de Julio de 2015. Consultado el 19 de octubre de 2015. <http://www.animalpolitico.com/2015/07/empresa-de-hackers-exhibida-por-venta-de-software-espia-a-paises-represores-y-mexico-resulta-su-principal-cliente/>
- Asociación por los Derechos Civiles. “Educar para Vigilar”. Diciembre de 2015. Consultado el 4 de enero de 2016. <https://adcdigital.org.ar/2016/01/29/educar-para-vigilar/>
- Barbara Partarrieu, y Matías Jara. “Los Correos Que Alertaron Sobre La Compra Del Poderoso Programa Espía De La PDI”. CIPER Centro de Investigación Periodística. 10 de julio de 2015. Consultado el 9 de marzo de 2016. <http://ciperchile.cl/2015/07/10/los-correos-que-alertaron-sobre-la-compra-del-poderoso-programa-espia-de-la-pdi/>
- Bill Marczak, Claudio Guarnieri, Morgan Marqui S - Boire, y John Scott - Railton. “Mapping Hacking Team’s ‘Untraceable’ Spyware”. Munk School of Global Affairs, 14, de febrero de 2014, 1-9. Consultado el 8 de noviembre de 2015. https://citizenlab.org/wp-content/uploads/2015/03/Mapping-Hacking-Team’s_-Untraceable_-Spyware.pdf
- Carlos Alberto Vargas. “Escuchas ilegales en el gobierno anterior. Triangularon compra de equipo para espionaje”. La Prensa Panamá. 27 de julio de 2015. Consultado el 19 de septiembre de 2015. http://www.prensa.com/politica/Traingularon-compra-equipo-espionaje_0_4264823642.html
- Comunicado de Prensa. “CIDH Publica Informe sobre la Situación de Derechos Humanos en México”. Organización de los Estados Americanos. 2 de marzo de 2016. Consultado el 10 de marzo de 2016. <https://www.oas.org/es/cidh/prensa/Comunicados/2016/023.asp>
- Corra Courier, y Morgan Marquis-Boire. “Secret Manuals Show the Spyware Sold to Despots and Cops Worldwide”. The Intercept. 30 de octubre de 2014. Consultado el 8 de febrero de 2016. <https://theintercept.com/2014/10/30/hacking-team/#manuals>
- Council of Europe. “Convenio sobre la Ciberdelincuencia”. 23 de septiembre de 2001. Consultado el 4 de marzo de 2016. https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF
- Daniel Coronell. “Los Caballeros de la Noche”. Semana. 5 de diciembre de 2015. Consultado el 10 de marzo de 2016. <http://www.semana.com//opinion/articulo/daniel-coronell-el-caso-del-general-palomino-la-banda-de-prostitucion-en-la-policia/452337-3>
- Daniel Salgar Antolínez. “Un Mundo De Chuzadas”. El Espectador. 22 de julio de 2015. Consultado el 28 de febrero de 2016. <http://www.elespectador.com/noticias/elmundo/un-mundo-de-chuzadas-articulo-574325>
- Dennys Antonialli, y Jacqueline De Souza Abreu. “Vigilância Das Comunicacões Pelo Es-

- tado Brasileiro E a Proteção a Direitos Fundamentais”. Electronic Frontier Foundation e Internet Lab, 2015, 11-12. Consultado el 9 de febrero de 2016. http://www.internetlab.org.br/wp-content/uploads/2015/11/VigilanciaEstado_Diagram_vprova.pdf
- Diana Carolina Durán Nuñez. “El Software Espía De La Policía”. El Espectador. 11 de julio de 2015. Consultado el 9 de marzo de 2016. <http://www.elespectador.com/noticias/investigacion/el-software-espia-de-policia-articulo-571980>
- EFE. “Julian Assange Cumple Tres Años Recluido en la Embajada de Ecuador en Londres”. 20minutos. 19 de junio de 2015. Consultado el 10 de noviembre de 2015. <http://www.20minutos.es/noticia/2493292/0/julian-assange/tres-anos/embajada-ecuador-londres/>
- Elizabeth Gonzalez. “Explainer: Hacking Team’s Reach in the Americas”. Americas Society Council of the Americas. 30 de Julio de 2015. Consultado el 10 de octubre de 2015. <http://www.as-coa.org/articles/explainer-hacking-teams-reach-americas-0>
- Elizabeth González. “Explainer: Hacking Team’s Reach in the Americas”. Americas Society Council of the Americas. 30 de Julio de 2015. Consultado el 15 de septiembre de 2015. <http://www.as-coa.org/articles/explainer-hacking-teams-reach-americas-0>
- Ernesto Aroche. “El gobierno de Puebla usó el software de Hacking Team para espionaje político”. Animal Político. 22 de julio de 2015. Consultado el 19 de octubre de 2015. <http://www.animalpolitico.com/2015/07/el-gobierno-de-puebla-uso-el-software-de-hacking-team-para-espionaje-politico/>
- Fabrizio Scrollini, Ana Tudurí, y Katitza Rodríguez. “Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Uruguay”. Electronic Frontier Foundation. Diciembre de 2015. Consultado el 15 de enero de 2016. <https://www.eff.org/es/country-reports/Uruguay-ES-final>
- Félix Palazuelos. “Hacking Team: Todo el Internet de Colombia Interceptado”. Hipertextual. 7 de julio de 2015. Consultado el 23 de septiembre de 2016. <http://hipertextual.com/2015/07/colombia-hacking-team>
- Frank Bajak, and Raphael Satter. “Ecuador: Hacking The Opposition”. Associated Press. 7 de agosto de 2015. Consultado el 18 de septiembre de 2015. <http://bigstory.ap.org/article/6f41d49888174b45857d34511fda1caf/apnewsbreak-email-leak-suggests-ecuador-spied-opposition>
- Frank Bajak. “South America Hacker Team Targets Dissidents, Journalists”. The Big Story. 9 de diciembre de 2015. Consultado el 8 de marzo de 2016. <http://bigstory.ap.org/article/fa7618cf36a642fb900a4f35b2c986b1/south-america-hacker-team-targets-dissidents-journalists>
- Fundación Karisma. “Sobre Hacking Team En Colombia”. 24 de julio de 2015. Consultado el 6 de enero de 2016. <https://karisma.org.co/sobre-hacking-team-en-colombia/>

- Fundamedios. “Senain Advierte con Tomar Acciones Legales por Divulgar Información que la Relacionan con Hacking Team”. 16 de julio de 2015. Consultado el 10 de octubre de 2016. <http://www.fundamedios.org/alertas/senain-advier-te-con-tomar-acciones-legales-por-divulgar-informacion-que-la-relacionan-con-hacking-team/>
- Glen Greenwald. “EUA Espionaram Milhões De E-mails E Ligações De Brasileiros”. O Globo. 12 de julio de 2013. Consultado el 9 de marzo de 2016. <http://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934>
- Gonzalo Terra. “Gobierno de Mujica sondeó compra de más equipos de espionaje”. El País Uruguay. 10 de julio de 2015. Consultado el 2 de febrero de 2016. <http://www.elpais.com.uy/informacion/gobierno-mujica-sondeo-compra-mas.html>
- Graeme Burton. “Did Hacking Team design software that could plant child porn on suspects’ PCs?” Computing. 6 de Julio de 2015. Consultado el 5 de marzo de 2016. <http://www.computing.co.uk/ctg/news/2416521/did-hacking-team-sell-software-to-plant-child-porn-on-suspects-pcs>
- Irina Hauser. “No sólo un cambio de manos”. Página 12. 7 de julio de 2015. Consultado el 4 de agosto de 2015. <http://www.pagina12.com.ar/diario/elpais/1-276542-2015-07-07.html>
- Jineth Bedoya Lima. “Guerra Contra el Narcotráfico: 20 Años de Dolor, Muerte y Corrupción”. El Tiempo. 24 de noviembre de 2013. Consultado el 9 de enero de 2016. <http://www.eltiempo.com/archivo/documento/CMS-13218657>
- Juan Diego Castañeda. “Cuando el Estado Hackea: Análisis de la Legitimidad del Uso de Herramientas de Hacking en Colombia”. Fundación Karisma. 10 de diciembre de 2015. Consultado el 15 de enero de 2015. <https://karisma.org.co/wp-content/uploads/2015/12/CUANDO-EL-ESTADO-HACKEA-D.pdf>
- Justicia. “Policía Indicó No Tener Vínculos Comerciales Con Firma Hacking Team”. El Tiempo. 8 de julio de 2015. Consultado el 9 de marzo de 2016. <http://www.eltiempo.com/politica/justicia/policia-indico-no-tener-vinculos-comerciales-con-firma-hacking-team/16063640>
- Katherine Pennacchio. “Hacking Team casi Corona en Venezuela”. Armando Info. 18 de julio de 2015. Consultado el 19 de octubre de 2015. [http://www.armando.info/sitio/index.php?id=17&tx_ttnews\[tt_news\]=158&cHash=465c7aebd69ddc598ea041c78d4cf5ae](http://www.armando.info/sitio/index.php?id=17&tx_ttnews[tt_news]=158&cHash=465c7aebd69ddc598ea041c78d4cf5ae)
- Katitza Rodríguez, Marlon Hernández Anzora, Hedme Sierra-Castro, Jorge Jiménez Barrillas, Edy Tábor González, y Mireya Zepeda Rivera. “¿Privacidad digital para defensores y defensoras de derechos humanos?” Consultado el 19 de enero de 2016. <http://acceso.or.cr/files/Investigacion-Privacidad-Digital-FA.pdf>
- Leandro Uciferri. “Hacking Team y sus planes para hackear en Argentina”. Tecnovortex. 10 de julio de 2015. Consultado el 18 de octubre de 2015. <http://tecnovortex.com/hacking-team-argentina/>

- Lee Fang. "Former AK-47 Dealer Goes Cyber, Supplied Surveillance Tools to Honduras Government". The Intercept. 27 de julio 2015. 9 de marzo de 2016. <https://theintercept.com/2015/07/27/ak-47-arms-dealer-goes-cyber-supplied-surveillance-tools-honduras-government/>
- Lorenzo Franceschi-Biccieri. "Hacking Team's Equipment Got Stolen in Panama". Motherboard VICE. 7 de julio de 2015. Consultado el 4 de agosto de 2015. <https://motherboard.vice.com/read/hacking-teams-equipment-got-stolen-in-panama>
- Luis Fernando García. "Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en México". Electronic Frontier Foundation. Octubre de 2015. Consultado el 19 de diciembre de 2015. <https://www.eff.org/node/89090>
- Manish Singh. "Hacking Team, Boeing Worked on Drones That Infect Computers Over Wi-Fi". 23 de julio de 2015. Consultado el 19 de agosto de 2015. <http://gadgets.ndtv.com/internet/news/hacking-team-boeing-worked-on-drones-that-infect-computers-over-wi-fi-719033>
- Martín Becerra. "Restauración". QUIPI- Políticas y Tecnologías de Comunicación. 14 de enero de 2016. Consultado el 18 de febrero de 2016. <https://martinbecerra.wordpress.com/2016/01/14/restauracion/>
- Mauricio Romero. "Cisen: 2 mil 74 solicitudes para espiar con tecnología de Hacking Team". Contralínea. 6 de marzo de 2016. Consultado el 10 de marzo de 2016. <http://www.contralinea.com.mx/archivo-revista/index.php/2016/03/06/cisen-2-mil-74-solicitudes-para-espiar-con-tecnologia-de-hacking-team/>
- Max Webber. "La Política Como Vocación". El Político y el Científico. Alianza Editorial; 2. 1919.
- Morgan Marquis-Boire, John Scott - Railton, Claudio Guarnieri, y Katie Kleemola. "Police Story: Hacking Team's Government Surveillance *Malware*". Munk School of Global Affairs, Junio 2014, 2-25. Consultado el 23 de septiembre de 2015. <https://citizenlab.org/wp-content/uploads/2015/03/Police-Story-Hacking-Team's-Government-Surveillance-Malware.pdf>
- Morgan Marquis-Boire. "You Can Get Hacked Just By Watching This Cat Video on YouTube". The Intercept. 15 de agosto de 2015. Consultado el 25 de agosto de 2015. <https://theintercept.com/2014/08/15/cat-video-hack/>
- Natalia Viana. "Em Parceria Com PF, Empresa De Software Espião Estaria Hackeando O Brasil - Notícias - Tecnologia". UOL Notícias. 28 de julio de 2015. Consultado el 9 de marzo de 2016. <http://tecnologia.uol.com.br/noticias/redacao/2015/07/28/em-parceria-com-pf-empresa-de-software-espiao-estaria-hackeando-o-brasil.htm>
- Natalia Viana. "Hackeando O Brasil". Pública. 27 de julio de 2015. Consultado el 8 de febrero de 2016. <http://apublica.org/2015/07/hackeando-o-brasil/>

- Pilar Sáenz, y Carolina Botero. “En Colombia, El PUMA No Es Como Lo Pintan”. Digital Rights LAC. Agosto 2014. Consultado el 15 de febrero de 2016. <http://www.digitalrights-lac.net/es/en-colombia-el-puma-no-es-como-lo-pintan/>
- Principios Rectores sobre las empresas y los derechos humanos: puesta en práctica del marco de las Naciones Unidas para “proteger, respetar y remediar”. Informe del Representante Especial del Secretario General para la cuestión de los derechos humanos y las empresas transnacionales y otras empresas, John Ruggie. Consejo de Derechos Humanos. 17º período de sesiones. Consultado el 10 de octubre de 2015. <http://www.global-business-initiative.org/wp-content/uploads/2012/07/GPs-Spanish.pdf>
- Privacy International. “Un Estado En La Sombra: Vigilancia Y Orden Público En Colombia”. Informe Especial, agosto de 2015. Consultado el 4 de enero de 2016. https://www.privacyinternational.org/sites/default/files/ShadowState_Espanol.pdf
- Raúl Kollman. “A un año de la muerte de Nisman: Una trama de operaciones políticas y judiciales”. 17 de enero de 2016. Consultado el 20 de enero de 2016. <http://www.pagina12.com.ar/diario/elpais/1-290509-2016-01-17.html>
- Redação Linha Defensiva. “Linha Defensiva”. PF Estava Para Fechar Contrato Milionário De Espionagem. 27 de julio de 2015. Consultado el 9 de febrero de 2016. <http://www.linhadefensiva.org/2015/07/pf-estava-para-fechar-contrato-milionario-de-espionagem/>
- Redacción de la Prensa. “10 claves para entender el caso de Hacking Team en Panamá”. La Prensa. 11 de julio de 2015. Consultado el 9 de agosto de 2015. http://www.prensa.com/politica/claves-entender-Hacking-Team-Panama_0_4251324994.html#sthash.ljl-zx37N.dpuf
- Redacción. “Acusa R3D a Jalisco de comprar programa espía a ‘Hacking Team’”. Aristegui Noticias. 9 de Julio de 2015. Consultado el 18 de septiembre de 2015. <http://aristeginoticias.com/0907/mexico/acusa-r3d-a-jalisco-de-comprar-programa-espia-a-hacking-team/>
- Redacción. “La Corte postergó la aplicación de otro ‘decreto de necesidad y urgencia’ de Macri”. Página 12. 29 de diciembre de 2015. Consultado el 14 de enero de 2016. <http://www.pagina12.com.ar/diario/ultimas/20-289216-2015-12-29.html>
- Redacción. “La muerte de Alberto Nisman”. Curaduría La Nación. Enero 2015. Consultado el 14 de febrero de 2016. <http://www.lanacion.com.ar/la-muerte-de-alberto-nisman-t53089>
- Redacción. “Macri transfirió las escuchas telefónicas a la Corte Suprema con un DNU”. Telam. 29 de diciembre de 2012. Consultado el 14 de enero de 2016. <http://www.telam.com.ar/notas/201512/131473-escuchas-corte-dnu.html>
- Redacción. “Osorio Chong dice que México compró software a Hacking Team en el gobierno de Calderón”. Sin Embargo. 7 de Julio de 2015. Consultado el 18 de septiembre de 2015. <http://www.sinembargo.mx/07-07-2015/1405444>

Reglamento de la Ley Orgánica de Petróleos Mexicanos. Publicado el 10 de Agosto de 1972. Consultado el 18 de diciembre de 2015. http://www.pemex.com/acerca/marco_normativo/Documents/reglamentos/REG_LEY_ORGANICA_PEMEX.pdf

Relator Especial de las Naciones Unidas 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”. Organización de los Estados Americanos. Consultado el 15 de enero de 2015. <https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=926&lID=2>

Rolando Rodríguez, y Juan Manuel Díaz. “Abren sumario en caso Hacking Team”. La Prensa Panamá. 7 de agosto de 2015. Consultado el 16 de octubre de 2015. http://www.prensa.com/locales/Espiar-obsesion-Martinelli_0_4271572998.html

Secretaría de Planeación y Finanzas. Gobierno de Baja California. Artículo 24. Consultado el 18 de diciembre de 2015. <http://www.bajacalifornia.gob.mx/portal/gobierno/dependencias/spf.jsp>

Steve Ragan. “Hacking Team Hacked, Attackers Claim 400GB in Dumped Data”. CSO. 5 de julio de 2015. Consultado el 8 de octubre de 2015. <http://www.csoonline.com/article/2943968/data-breach/hacking-team-hacked-attackers-claim-400gb-in-dumped-data.html>

Tabatha Molina. “Panamá pesquisa gestión de Martinelli por caso Hacking Team”. Panam Post. 10 de agosto de 2015. Consultado el 14 de agosto de 2015. <http://es.panam-post.com/thabata-molina/2015/08/10/panama-investigara-a-martinelli-porescandalo-de-hacking-team/>

E-MAILS DE HACKING TEAM

A.scarafite@hackingteam.it. “Argentina-Hilton Demonstrations Schedule”. E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/593799>

A.scarafite@hackingteam.it. “Argentina”. E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/765194>

A.velasco@hackingteam.it. “Meetings in Argentina”. E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/611846>

A.velasco@hackingteam.it. “Report on Argentina visit with final agenda attached”. E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/596983>

Alex.lawson@globalinteractivegroup.com. “RE: Att. Eduardo Pardo y Massimiliano Luppi Rtt. Alex Lawson”. E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/433276>

Alex.lawson@globalinteractivegroup.com. “RE: Att. Eduardo Pardo y Massimiliano Luppi

Rtt. Alex Lawson". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/433277>

Aristeosanchez@gmail.com. "Re: Propuesta". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/249820>

D.milan@hackingteam.com. "Fwd: Guatemala delivery". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/517846>

D.vincenzetti@hackingteam.com. "Brenda Operation". E-mail. 8 de Julio de 2015. Wikileaks. <https://www.wikileaks.org/hackingteam/emails/emailid/921908>

D.vincenzetti@hackingteam.com. "FWD: Guatemala". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/173519>

G.russo@hackingteam.com "Re: (Global Interactive Group) NDA & Partner PolicyE-mail". 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/407300>

G.russo@hackingteam.com. "Fwd: Re: hardware requirements". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/446475>

Ivan.sanchez@nullcode.com.ar. "Product Remote Control System". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/4135>

Luca.gabrielli@9isp.com.br. "Intrusão e controle para smartphone". E-mail. 8 de Julio de 2015. Wikileaks. <https://www.wikileaks.org/hackingteam/emails/emailid/440433>

Luca.gabrielli@yasnitech.com.br. "Pagamento e programmazione". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/7014>

Luca.gabrielli@yasnitech.com.br. "Progetto Polizia Federal". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/6963>

Luca.gabrielli@yasnitech.com.br. "Proposta para piloto HT". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/439854>

M.bettini@hackingteam.it. "Re: Plan Q1". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/3195>

M.bettini@hackingteam.it. "Resoconto Argentina". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/805712>

M.luppi@hackingteam.com. "Defense Tech / HT - Business in Brazil - Your best attention" E-mail. 8 de Julio de 2015. Wikileaks. <https://www.wikileaks.org/hackingteam/emails/emailid/7226>

M.luppi@hackingteam.com. "I: Guatemala payment". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/455941>

M.luppi@hackingteam.com. "Opportunity Argentina". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/4517>

M.luppi@hackingteam.com. "R: Guatemala". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/446530>

M.luppi@hackingteam.com. "RE: Att. Eduardo Pardo y Massimiliano Luppi Rtt. Alex Lawson". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/434521>

M.luppi@hackingteam.com. "Update Guatemala". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/5071>

M.luppi@hackingteam.it. "Meetings in Argentina". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/600077>

M.russo@wiseplant.com. "Product Remote Control System". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/4526>

M.russo@wiseplant.com. "Product Remote Control System". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/138576>

P.vinci@hackingteam.com. "Re: NICOLAS>>(Tamce) Meeting". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/1088185>

S.solis@hackingteam.it. "Paraguay-Uruguay Report". 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/455941>

Support@hackingteam.it. "Exploit Docx". E-mail. 8 de Julio de 2015. Wikileaks <https://wikileaks.org/hackingteam/emails/emailid/529235>

Support@hackingteam.it. "Exploit Requests". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/640759>

Support@hackingteam.it. "HTML Exploit". E-mail. 8 de Julio de 2015. Wikileaks <https://wikileaks.org/hackingteam/emails/emailid/532912>

Vince@hackingteam.com. "Status Solution RCS Panama". E-mail. 8 de Julio de 2015. Wikileaks. <https://wikileaks.org/hackingteam/emails/emailid/600077>

