Cuando el Estado "hackea"[1]*

Análisis de la legitimidad del uso de herramientas de hacking en Colombia

Fundación Karisma

Por, Juan Diego Castañeda

Un Fiscal argentino recibe un archivo PDF en su correo electrónico llamado "estrictamente secreto y confidencial.pdf" y por suerte, intenta abrirlo en su teléfono Android. Si lo hubiera abierto en su computador "el archivo no habría mostrado más que una página en blanco. Mientras [el Fiscal] piensa en qué significa esto, un software espía se habría instalado en su máquina"[2]. Un periodista colombiano está investigando un caso de corrupción en la Policía cuando "de un momento a otro sonó el teléfono y vio cómo la flecha del mouse se empezó a mover sola, como si estuviera poseída o controlada remotamente y eliminó el documento"[3] en el que estaba trabajando. Estos casos demuestran que las comunicaciones hoy no solo pueden ser censuradas o interceptadas, también pueden ser afectadas por ataques informáticos, pues los dispositivos que usamos a diario son vulnerables y guardan mucha información personal que puede ser interesante para el atacante.

Internet está siendo afectado por todo tipo de medidas de control que determinan hasta qué punto es un medio libre, abierto y seguro. Ron Deibert clasifica los controles de la siguiente forma[4]. La primera generación de controles consiste en sistemas de defensivos de filtrado o bloqueo de contenidos. La segunda generación nace de la colaboración de los gobiernos con el sector privado, imponiendo o solicitando acceso a "puertas traseras" en el hardware o

---

[1] * "Hackear" es una expresión que identifica una ética que consiste en propiciar el acceso a la tecnología para empoderar a las personas, luego se entendió como la actividad de encontrar vulnerabilidades en sistemas de información pero esencialmente con la idea de reportarlas y repararlas. Finalmente se empezó a usar en el sentido de buscar vulnerabilidades en sistemas de información y aprovecharlas en forma ilícita. Para Karisma la expresión correcta de la última ascepción es "crackear" y por tanto utilizar la expresión "hackear" en ese sentido es incorrecto, sin embargo ese uso de la palabra es el que se ha popularizado. Para facilitar la comprensión del documento, hemos decidido usar el término "hackear" en el sentido de "crackear" aunque somos conscientes de que con eso ayudamos a estrechar el significado de esa palabra que es mucho más amplio e interesante.

[2] Marquis-Boire M. "Inside the spyware campaign against argentine troublemakers". The Intercept, 21 de agosto de 2015. Recuperado de https://theintercept.com/2015/08/21/inside-the-spyware-campaign-against-argentine-troublemakers-including-alberto-nisman/

[3] Vélez, L. "El precio de denunciar". El Espectador, 6 de diciembre de 2015. Recuperado de http://www.elespectador.com/opinion/el-precio-de-denunciar

[4] Deibert, R. (2015). Cyberspace under siege. J*ournal of Democracy*, 26(3).

software, estableciendo mayores requisitos para el acceso a Internet, como el registro con datos biométricos, o prohibiendo el uso de herramientas de seguridad y cifrado.

Los controles de tercera generación son ofensivos e incluyen el uso de ataques dirigidos por parte de los gobiernos, a través de capacidades propias o empleando tecnologías del sector privado como las que ofrece la empresa Hacking Team. Los Estados, entonces, han estado adquiriendo capacidades tecnológicas para acceder subrepticiamente a dispositivos electrónicos y obtener información de ellos, e incluso encender las cámaras o los micrófonos y registrar lo que ellos perciben[5], es decir, para hackearlos con propósitos que Venezuela y Paraguay[6]. De otra parte, desde febrero de 2014, gracias a otra investigación del CitizenLab, se conoce del uso de un malware comercializado por Hacking Team en por los menos tres países de la región: México, Panamá y Colombia[7]. Las revelaciones de 2015 sobre las filtraciones a la empresa italiana Hacking Team confirmaron esa investigación, e incluso se estableció que la extensión del uso de esta herramienta en la región era mucho mayor de lo reportado inicialmente[8]. Se supo también que Ecuador, Chile y Honduras, en algún momento, habían adquirido o utilizado este software[9], que Brasil había conseguido las autorizaciones correspondientes para usarlo y pensaba utilizarlo como mecanismo de vigilancia en las próximas olimpiadas[10], que en Perú se realizaron demostraciones[11], y que en Argentina también se estaban haciendo avan desde la investigación criminal hasta la supresión de la disidencia, pasando por la recopilación de información para inteligencia[12].

---

[5] LaRue, F. (2013). *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión*. A/HRC/23/40,p. 37.

[6] Marczak, B. et al. (2015, 15 de octubre). *Pay no attention to the server behind the proxy: mapping FinFisher's continuing proliferation*. Toronto, Canadá: CitizenLab. Recuperado de https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/.

[7] Marczak, B. et al. (2014). Mapping Hacking Team's "untraceable" spyware. Toronto, Canadá: Citizen Lab, p. 17. Recuperado de https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/.

[8] Cuando hackean a los hackers (2015, 11 de julio). *Revista Semana*. Recuperado de http://www.semana.com/nacion/articulo/los-lios-de-hacking-team-por-informacion-hackeada/434391-3

[9] Fundación Karisma (2015, 7 de julio). *Sociedad civil de América Latina rechaza software espía de Hacking Team*. Recuperado de https://karisma.org.co/sociedad-civil-de-america-latina-rechaza-software-espia-de-hacking-team/.

[10] Viana, N. (2015, 27 de julio). Hackeando o Brasil. *Agencia Pública*. Recuperado de http://apublica.org/2015/07/hackeando-o-brasil/.

[11] Vinculan a entidades del Estado con empresa de espionaje Hacking Team (2015, 12 de julio). *RPP noticias*. Recuperado de http://rpp.pe/politica/actualidad/vinculan-a-entidades-del-estado-con-empresa-de-espionaje-hacking-team-noticia-816283.

[12] *Véase*, por ejemplo, McCullagh, D. (2007). *Feds use keylogger to thwart PGP, Hushmail. CNET*. Recuperado de http://www.cnet.com/news/feds-use-keylogger-to-thwart-pgp-hushmail/; Nagaraja, S., & Anderson, R. (2009). T*he snooping dragon: social-malware surveillance of the Tibetan movement. University of Cambridge Computer Laboratory;* Glance, D. (2011, 11 de octubre). Ein spy: is the German government using a trojan to watch its citizens? *The Conversation*. Recuperado de https://theconversation.com/ein-spy-is-the-german-government-using-a-trojan-to-watch-its-citizens-3765-.

El uso que Estados y privados hacen de estas herramientas suponen un problema para el ejercicio de derechos humanos pues implica una intromisión total en la vida íntima de la persona objetivo y por tanto puede afectar, entre otros, el derecho a la libertad de expresión. Aunque estas herramientas han hecho presencia no sólo en Colombia sino también en varios países de Latinoamérica, no ha habido un debate sobre su legitimidad ni sobre los retos que estas actividades suponen para los marcos legales de derechos humanos en nuestros países.

De otra parte, se afirma que el uso de estas herramientas por parte de las autoridades de vigilancia es una necesidad para la lucha contra el crimen y el terrorismo, pues iguala las capacidades de la delincuencia con las de la autoridad[13]. Incluso, hay quienes sostienen que el uso de herramientas de hackeo puede ser legítimo en la medida que exista una orden judicial para aprovechar vulnerabilidades de sistemas informáticos. La legalización y aplicación de controles judiciales a esta actividad podría tener el efecto de ponerle límites, así como minimizar sus efectos negativos. Esta alternativa evitaría la creación de nuevas vulnerabilidades, pues solo explota las que ya existen y aliviaría la presión sobre fabricantes o prestadores de servicios para colaborar con los gobiernos[14]. Sin embargo, éstas son discusiones que no han ocurrido en nuestro país y que merecen atención.

Hacking Team en América Latina

En América Latina, solo hasta el 2015, la ciudadanía estableció que las herramientas de hackeo forman parte del portafolio de actividades de las autoridades de vigilancia de la región.

En marzo de 2013, un informe del CitizenLab documenta por primera vez el uso del software Finfisher en México[15]. Poco después, en abril del mismo año, un nuevo informe de esa organización mostraba la ampliación de su uso a Panamá[16]. En el último reporte de octubre de 2015, el CitizenLab muestra como Finfisher está siendo utilizada también por cercamientos[17].

---

[13] Vincenzetti, D. (2015, 29 de julio). Terrorists and criminals have a lot less to worry about since we were hacked. *International Business Times*. Recurperado de: http://www.ibtimes.co.uk/hacking-team-ceo-terrorists-criminals-have-lot-less-worry-about-since-we-were-hacked-1513148. Vicenzetti es el CEO de la compañía italiana Hacking Team.

[14] Bellovin S.M., et al. (2014). Lawful hacking: using existing vulnerabilities for wiretapping on the internet. *Northwestern Journal of Technology and Intellectual Property*. 12, p. 1. Recuperado de http://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1.

[15] Marquis-Boire, M. et al. (2013). *For their eyes only: the commercialization of digital spying*. Toronto: Canadá: Citizen Lab. Recuperado de https://citizenlab.org/2013/04/for-their-eyes-only-2/.

[16] Marquis-Boire, M. et al. . (2013). *You only click twice: FinFisher's global proliferation*. Toronto, Canadá: University of Toronto. Recuperado de https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/.

[17] Dubove, A (2015, 13 de julio). Hacking Team hizo contactos en Argentina para vender software espía. *Panam Post*. Recuperado de http://es.panampost.com/adam-dubove/2015/07/13/hacking-team-hizo-contactos-en-argentina-para-vender-software-espia/.

La reacción de los gobiernos de la región ante estas revelaciones ha sido diversa. La Secretaría Nacional de Inteligencia de Ecuador negó su relación con Hacking Team[18]. No obstante, existen pruebas que sugieren el uso de su software contra personas y grupos opositores[19]. En Chile, la Policía de Investigaciones admitió la adquisición del software de Hacking Team y justificó la compra como parte de los proyectos de modernización "cuyo objetivo era incrementar sus capacidades operativas en la investigación de crimen organizado, terrorismo internacional y narcotráfico a gran escala"[20].

Finalmente, en México, tras las filtraciones, se comprobó que 14 autoridades, tanto federales como estatales, eran clientes de la firma italiana y se cuestionó la legalidad de estas actividades[21]. Según los documentos filtrados, el país realizó el mayor pago que se haya hecho de alguna corporación pública o privada en la historia de la compañía, al adquirir 600 licencias para realizar monitoreos simultáneos[22].

Herramientas de hackeo en Colombia

La filtración de correos de la empresa italiana Hacking Team confirmó que en Colombia se había comercializado su sistema de control remoto y que probablemente se estaría usando. El comprador resultó ser la Dirección Nacional de la Policía (DIPON). En un comunicado a medios de comunicación, la Policía no negó el uso de los productos de Hacking Team pero rechazó tener relaciones con esta empresa. También afirmó que no ha sostenido vínculo comercial con la firma Hacking Team, aunque admitió que "adquirió una herramienta tecnológica con la empresa Robotec Colombia S.A.S, que ofrece equipos para la seguridad.

---

[18] Secretaría Nacional de Inteligencia niega contratos con empresa que ofrece servicios de espionaje (2015, 10 de julio). *El Universo*. Recuperado de http://www.eluniverso.com/noticias/2015/07/10/nota/5011474/secretaria-inteligencia-niega-contratos-empresa-que-ofrece.

[19] APNewsBreak: leaked Hacking Team emails suggest Ecuador illegally spied on opposition (2015, 6 de agosto). *US New*. Recuperado de http://www.usnews.com/news/business/articles/2015/08/06/apnewsbreak-email-leak-suggests-ecuador-spied-on-opposition.

[20] PDI confirma compra de software creado por empresa italiana que fue hackeada (2015, 6 de julio).. *El Mercurio*. Recuperado de http://www.emol.com/noticias/Tecnologia/2015/07/06/724738/PDI-confirma-compra-de-software-creado-por-empresa-italiana-que-fue-hackeada.html.

[21] Sánchez, J. (2015, 6 de julio).Vulneración a Hacking Team confirma abuso de espionaje en México. *El Economista*. Recuperado de http://eleconomista.com.mx/tecnociencia/2015/07/06/vulneracion-hacking-team-confirma-abuso-espionaje-mexico.

[22] Ángel, A. (2015, 21 de julio). Sedena negoció compra de software a Hacking Team en 2015 para espiar a 600 personas. *Animal Político*. Recuperado de http://www.animalpolitico.com/2015/07/sedena-negocio-compra-de-software-a-hacking-team-en-2015-para-espiar-a-600-personas/.

El propósito de esta compra –dijo– fue potencializar la capacidad de detección de amenazas del terrorismo y la criminalidad organizada en el ciberespacio colombiano[23]".

Lo que adquirió la Policía fue el sistema de control remoto llamado "Galileo" que se instala en el dispositivo objetivo a través de archivos especialmente diseñados para la persona que los controla los abra, permitiendo así al atacante tomar control del aparato, para sustraer información, acceder al micrófono o a la cámara web e incluso a lo que se escribe en el teclado[24].

En un primer caso donde se sospecha el uso de herramientas de hackeo, el 3 de diciembre pasado el Fiscal General de la Nación anunció el inicio de la investigación por la denuncia que presentó la periodista Vicky Dávila por supuestas interceptaciones de comunicaciones privadas suyas, de su familia y de su equipo de trabajo. El motivo de estos ataques contra periodistas parece ser el hecho de que poseen información filtrada la Policía que apunta a graves casos de corrupción e incluso a una supuesta red de prostitución que beneficiaría a los altos mandos de esa institución[25].

Aunque aparentemente también hubo seguimientos físicos ilegales[26], el periodista Juan Pablo Barrientos, que investigaba el escándalo en la Policía, fue el protagonista de la historia que presentamos en el primer párrafo. De repente, se borraron algunos archivos en los que estaba trabajando en su computador, no por accidente sino como si alguien hubiera tomado control del aparato.

Problemas del Hackeo

Tomar control de un dispositivo ajeno, sin importar el medio técnico que se emplee, equivale a una interceptación de comunicaciones y por tanto en Colombia se requiere que exista una ley que lo autorice y que haya control judicial de esa actividad[27]. Muchas de las herramientas con las que hoy cuentan las autoridades tienen, de alguna manera, un alcance limitado. La interceptación de llamadas o correos electrónicos extrae solo la información que cursa por esos medios y que la persona afectada ha decidido compartir con otras. En cambio, el acceso a un sistema informático, bien sea un computador personal o un teléfono móvil, puede implicar la recolección de toda clase de información personal como fotos, documentos de trabajo o personales, historial de navegación, acceso a micrófonos y cámaras web, e incluso al control mismo el dispositivo. Todo esto, sin que la persona se

---

[23] Policía Nacional niega vínculo con la firma Hacking Team (2015, 8 de julio). *W Radio.* Recuperado de http://www.wradio.com.co/noticias/actualidad/policia-nacional-niega-vinculo-con-la-firma-hacking-team/20150708/nota/2841301.aspx.

[24] Botero, C. & Sáenz, P. (2015, 24 de agosto)."En Colombia, el PUMA no es como lo pintan. Digital Rights Latin America & the Caribbean. Disponible en: http://www.digitalrightslac.net/es/en-colombia-el-puma-no-es-como-lo-pintan/.

[25] Coronell, D. (2015, 8 de diciembre). "Los caballeros de la noche". Revista Semana. Recuperado de: http://www.semana.com//opinion/articulo/daniel-coronell-el-caso-del-general-palomino-la-banda-de-prostitucion-en-la-policia/452337-3

[26] "El informante de las 'Chuzadas'" (2015, 7 de diciembre). *El Espectador*. Recuperado de: http://www.elespectador.com/noticias/investigacion/el-informante-de-chuzadas-articulo-604187

[27] Constitución Política de Colombia. Artículo 15.

entere o sin que pueda establecerse un límite temporal a la ejecución de la intrusión. El hackeo, claramente, entrega mucha más información que la que se obtendría, por ejemplo, en el allanamiento de la casa de la persona afectada, aunque, por contraste, para esta última medida existan muchos más controles que para la primera.

La intrusión en los dispositivos de las personas es una violación a su intimidad, pero también afecta su derecho a la libre expresión y opinión. Como afirma el Relator Especial de las Naciones Unidas (ONU) para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión, en la era digital, el ejercicio de estos derechos no se limita al fuero interno de las personas, también se ejerce en el uso de buscadores o en el almacenamiento de archivos que se encuentran en los dispositivos o en la nube[28].

El debate sobre la legalidad del hackeo en Colombia, sobre el eventual alcance de una ley que lo permita y la obligación de incluir en ella controles para evitar abusos, como por ejemplo establecer el control judicial previo, no son los único elementos ni constituyen los más altos estándares que existen actualmente para considerar que una restricción a derechos fundamentales como el hackeo es legítima. Para la Relatoría para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, la legitimidad de las medidas de vigilancia de las comunicaciones deriva del cumplimiento de ciertas condiciones decantadas de los distintos documentos del Sistema Interamericano de Derechos Humanos [29]. Estos requisitos son:

1. Consagración legal
2. Búsqueda de una finalidad imperativa
3. Necesidad, idoneidad y proporcionalidad de la medida para alcanzar la finalidad perseguida
4. Debido proceso y reserva judicial

El Relator para libertad de expresión de la OEA, a propósito de las revelaciones sobre el uso de productos y servicios de la empresa italiana Hacking Team por parte de gobiernos alrededor del mundo, expresó que:

> *de acuerdo con los estándares internacionales, el uso de programas o sistemas de vigilancia en las comunicaciones privadas debe estar establecido de manera clara y precisa en la ley, ser verdaderamente excepcional y selectivo, y estar limitado en función a lo estrictamente necesario para el cumplimiento de fines imperativos como la investigación de delitos graves definidos en la legislación*[30].

---

[28] Kaye, D (2015). Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/29/32, párr. 20. Recuperado de: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc

[29] CIDH (2013). Libertad de expresión e internet. OEA/Ser.L/V/II.149 Doc.50, Capítulo IV, párr. 55.

[30] Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA (2015, 21 de julio). Comunicado de prensa sobre la adquisición e implementación de programas de vigilancia por parte de Estados del hemisferio. Recuperado de http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=998&lID=2.

Finalmente, hay que tener en cuenta los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, que fueron desarrollados a partir de las conceptualizaciones que se han realizado en torno al derecho internacional de los derechos humanos en el entorno digital[31] en un proceso que distintas organizaciones de la sociedad civil lideraron y que contó con la participación de representantes de la industria y expertos en la materia. Los principios que deben regir la aplicación de medidas de vigilancia de las comunicaciones son: legalidad, objetivo legítimo, necesidad, idoneidad, proporcionalidad, autorización judicial competente, debido proceso, notificación del usuario, transparencia, supervisión pública, integridad de las comunicaciones y los sistemas, garantías para la cooperación internacional y garantías contra el acceso ilegítimo, y derecho a un recurso efectivo.

No existe todavía en ningún país de América Latina un marco legal para realizar la actividad de intrusión o 'hackeo' de dispositivos. Por tanto, el primer requisito de legalidad como garantía de legitimidad de una medida de restricción de derechos no está satisfecho. La existencia de una ley en sentido formal y material presupone un debate público sobre la necesidad, proporcionalidad e idoneidad de la medida, de ahí que pueda decirse que tampoco están cumplidos estos requisitos.

La actual ilegalidad del uso de herramientas de hackeo es más notoria si se tiene en cuenta que hay leyes que lo penalizan. En Colombia es delito el acceso abusivo a un sistema informático, la interceptación de datos informáticos y el uso de software malicioso, entre otros[32]. En Perú, se penaliza el acceso ilícito a sistemas informáticos y la interceptación de comunicaciones privadas[33]. En México es delito la intervención de comunicaciones privadas [34] y en Brasil se castiga la invasión de dispositivos informáticos[35]. A pesar de la aparente ilegalidad de las actividades que denunciaron los escándalos de Hacking Team, por lo menos en Colombia no hay investigaciones en contra de las personas o entidades responsables.

Conclusiones

Si se propusiera una norma para legalizar el uso de herramientas de hackeo por parte de las autoridades, dicha norma debería ser clara respecto a los tipos de herramienta que se pueden usar y las funciones del equipo que puede afectar, por ejemplo, el acceso a archivos guardados dentro del dispositivo, a registrar los que se teclea o a lo que perciben el micrófono o la cámara web. Asimismo, debe ser clara respecto a cuánto tiempo puede emplearse una herramienta semejante, qué autoridades y bajo qué condiciones puede hacerlo (p. ej. investigaciones de ciertos crímenes).

También debe analizarse hasta qué punto está limitada la medida en cuanto a los medios sobre los que operaría (redes, computadores personales, teléfonos móviles, cámaras de

[31] Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. Recuperado de https://es.necessaryandproportionate.org/text.
[32] Código Penal. Artículos 269A, 269C y 269E respectivamente.
[33] Ley No. 300096 (2013). Artículos 2 y 7 respectivamente.
[34] Código Penal Federal Artículo 177.
[35] Código Penal Artículo 154A.

seguridad, tráfico de internet, etc.), sobre los datos a los que accedería, y el tiempo máximo por el cual podría implementarse, sin olvidar que los motivos para emplear semejante facultad también debería estar limitado a algunos casos puntuales.

La falta de precisión en alguno de estos temas puede ser un cheque en blanco en favor de la autoridad que pueda desplegar la medida, de donde puede fallarse el requisito de objetivo legítimo, pues se permitiría una restricción de derechos por razones vagas y poco fundamentadas, y el requisito de necesidad y proporcionalidad.

Es claro que el hackeo requeriría autorización judicial, por tanto, debe establecerse un procedimiento de solicitud en el que se pueda comprobar la satisfacción de los requisitos que exigiría la ley para el uso de la medida y que, además, impida su abuso. También debe contener provisiones respecto a la observación de la cadena de custodia, la notificación de la persona afectada para que pueda ejercer el derecho a la defensa, y la presentación de informes de transparencia por parte de las autoridades sobre la frecuencia de uso y la efectividad de la medida.

Finalmente, hay que tener en cuenta que la medida de hackeo como una forma legítima de vigilancia de las comunicaciones puede contener una contradicción respecto a otros deberes del Estado. Por un lado, este tipo de medidas se basan en la existencia de vulnerabilidades informáticas, es decir, en fallas de seguridad. Por el otro, los Estados desarrollan actualmente políticas de ciberseguridad, siguiendo el deber que tienen de garantizar la seguridad de la ciudadanía. Si el Estado no reporta las vulnerabilidades que encuentra, mantiene condiciones de inseguridad contraviniendo sus obligaciones. Si las reporta, en cambio, reduce las oportunidades para usarlas, desperdiciando el tiempo y los recursos que empleó para explotarlas. La superación de esta contradicción es un tema que debe ser parte necesariamente de la discusión pública sobre la legalización del hackeo.

Consulta en línea este análisis https://karisma.org.co/cuando-el-estado-hackea-3/