Lima, 20 de septiembre de 2017

Señor
Jesús Eloy Espinoza Losada
Secretario Técnico
Comisión de Defensa de la Libre Competencia
Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual
Lima
Presente. —

Referencia: Carta No. 718-2017/ST-CLC-INDECOPI

Hiperderecho es una asociación civil peruana sin fines de lucro dedicada a investigar y promover el respeto de los derechos humanos en entornos digitales, conformada por abogados y especialistas en tecnología. Como parte de nuestro trabajo, estudiamos todas las iniciativas de política pública que puedan impactar el ejercicio de derechos y libertades en estos ámbitos.

Saludamos la disposición de su despacho de brindar información adicional sobre la Adjudicación Simplificada No. 003-2017-INDECOPI para la Adquisición de un Kit de Extracción y Transferencia de Evidencia Forense en Dispositivos Móviles y una Licencia de Software para Procesamiento y Análisis Forense de Evidencia en Dispositivos Móviles. Sin embargo, el contenido de su Carta nos indica que no hemos sido lo suficientemente claros en expresar nuestros comentarios iniciales.[1] Creemos que la ciber militarización de la administración pública es un problema merecedor de una conversación pública, abierta y sincera. En ese sentido, nos vemos en la obligación de precisar lo siguiente.

Nuestro artículo no contiene exageraciones, inexactitudes, ni afirmaciones maliciosas

1. Lo que la Comisión de Defensa de la Libre Competencia (en adelante, la Comisión) ha adquirido es un equipo (*hardware*) y la licencia para usar el programa (*software*) del referido equipo. Esta información está contenida en la propia carátula de las bases. Por ende, resulta incompleto referirse exclusivamente a un "software" como lo hacen los puntos 1, 2 y 3 de su Carta.

[1] Nos referimos a nuestro artículo "Indecopi ahora puede hackear nuestros celulares" publicado el 11 de septiembre de 2017 en el blog de la página web de nuestra organización. URL: http://hiperderecho.org/2017/09/indecopi-ahora-puede-hackear-celulares/ (https://perma.cc/4HC3-ZBSZ).

2. No ponemos en discusión la necesidad de eventualmente acceder a la información contenida en dispositivos móviles para la investigación y detección de cárteles previa autorización judicial. **Nuestro artículo cuestiona la pertinencia de que sea la Comisión la instancia gubernamental encargada de adquirir, custodiar y operar sofisticados equipos de extracción digital forense para tal fin.** A modo de analogía, señalábamos que la potestad de la Secretaría Técnica de solicitar judicialmente el levantamiento del secreto de las comunicaciones no la autorizaba a comprar equipos de interceptación telefónica como los de la Policía. En este caso, consideramos una genuina pregunta de política pública si las instancias administrativas (que como parte de su trabajo necesitan restringir derechos fundamentales) están autorizadas también a procurarse los instrumentos para hacerlo o si resulta deseable que así lo estén.
3. Su Carta confunde dos escenarios claramente distintos de vulneración del secreto de las comunicaciones: el **acceso a información en tránsito** (ej. interceptación de llamadas telefónicas) y el **acceso a información en reposo** (ej. copia de los mensajes de texto contenidos en un teléfono). El equipo UFED Touch 2 fabricado por Cellebrite y adquirido por su despacho sirve exclusivamente para acceder a información en reposo y nuestro artículo nunca afirma algo distinto.
4. Nuestro artículo afirma correctamente que el UFED Touch 2 sirve para "hackear" un dispositivo móvil. La mayoría de dispositivos móviles modernos tienen mecanismos de bloqueo de distintos grados, desde contraseñas numéricas de acceso hasta el cifrado por defecto de la información contenida. Lo que el UFED Touch 2 hace es ejecutar una serie de operaciones sobre el equipo conectado para acceder en forma automatizada a la información en él contenida. Para lograrlo, puede saltarse los mecanismos de seguridad impuestos o incluso romper el cifrado de ciertos dispositivos. Equipos como los que su despacho ha adquirido explotan vulnerabilidades conocidas en sistemas operativos antiguos y, muy posiblemente, también incorporen otras todavía no solucionadas que han sido desarrolladas por Cellebrite. Esta es una modalidad de "hacking" conocida como "cracking."[2] En otros términos, lo que hace es acceder a un sistema informático para extraer información. Si esta operación se llevara a cabo sin autorización judicial o permiso de titular del equipo, se configuraría el delito de Acceso Ilícito a un sistema informático.[3]

[2] El término "hackear" se usa genéricamente para referirse a cualquier forma de interacción con uno o más sistemas informáticos de manera no tradicional. Se trata de un término técnico y no es una calificación legal ni se refiere al delito informático de Acceso Ilícito. El uso de la palabra "hackear" está tan extendido en nuestra sociedad que incluso instituciones como el Ministerio de Salud o el Registro Nacional de Identidad y Estado Civil organizan "maratones de hackeo" o "hackatones."

[3] **Ley 30096, Artículo 2. — Acceso ilícito**

Su Carta tiene como objetivo despejar cualquier duda sobre los posibles usos excesivos o ilícitos que pueda dársele al equipo. Sin embargo, más allá de su promesa de no hacerlo, no presenta más evidencia al respecto.

5. Nos gustaría saber si es que existe algún reglamento, directiva o protocolo vigente en Indecopi que regule cómo se va custodiar y controlar el uso de este equipo cuando no esté siendo usado en visitas inspectivas. Idealmente, esta norma tendría que señalar un flujo de autorizaciones, oficinas responsables, régimen sancionatorio y reglas aplicables a la conservación y destrucción de la información obtenida. En particular, nos preocupa la posibilidad de que un sofisticado equipo de vigilancia electrónica pueda caer en las manos incorrectas o ser usado de manera inapropiada por agentes maliciosos que aprovechen la buena fe y los recursos de la institución. La Policía Nacional del Perú, por ejemplo, cuenta con Protocolos especiales y públicos para llevar a cabo procedimientos de esta naturaleza. ¿Existen reglas similares en Indecopi?
6. Nos gustaría saber si ustedes conocen de otras autoridades de competencia de naturaleza administrativa con funciones similares a la de la Comisión que hayan adquirido directamente en el pasado equipos de esta naturaleza. Como señalábamos al inicio de esta comunicación, no cuestionamos la necesidad de realizar estas actividades sino la pertinencia de que sea la propia Secretaría Técnica quien adquiera, custodie y opere estos equipos que, por su naturaleza, deben de ser operados con la mayor cautela. ¿Es regular que autoridades de la competencia adquieran sofisticados equipos forenses para operarlos directamente?

Sin más, le expresamos nuestros mejores deseos y mayor consideración.

Atentamente,

Miguel Morachimo Rodríguez
Director Ejecutivo

Asociación Civil Hiperderecho
Jr. Colina 107, Barranco, Lima 15063
RUC: 20551193099

El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.
Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado.