REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA

VOL. 8 NÚM. 2 (2019) • PÁGS. 83-110 • DOI 10.5354/0719-2584.2019.54436
RECIBIDO: 16/9/2019 • APROBADO: 26/11/2019 • PUBLICADO: 31/12/2019

DOCTRINA

Cuando el Estado hackea: El caso de Operación Huracán

When the state is the hacker: A study case of Operación Huracán

Pablo Viollier Bonvin
Universidad Diego Portales, Chile

Valeria Ortega Romo
Abogada independiente, Chile

RESUMEN El trabajo analiza la legalidad de la utilización de técnicas de *hacking* por parte de la Dirección de Inteligencia de Carabineros de Chile (Dipolcar), a la luz de los hechos ocurridos en la polémica Operación Huracán. Para ello, se hace una breve relación de las herramientas y técnicas que eventualmente podrían permitir obtener acceso a las comunicaciones de aplicaciones como Whatsapp y Telegram. Luego, se estudian las normas del Código Procesal Penal y la Ley 19.974, a fin de evaluar si estos cuerpos habilitan a las policías para acceder a sistemas informáticos, infectar dispositivos con programas maliciosos y utilizar técnicas de *phishing*. Por último, se entregan breves recomendaciones para que una futura modificación de la ley de inteligencia permita adecuarla a estándares internacionales de derechos humanos.

PALABRAS CLAVE Privacidad, ciberseguridad, *hacking* estatal, derechos humanos, delitos informáticos.

ABSTRACT The paper analyzes the legality of hacking operations carried out by the Dirección de Inteligencia de Carabineros de Chile (Dipolcar) during the controversial "Operación Huracán". In order to achieve this objective, a brief description of the tools and techniques that could eventually allow access to communications from applications such as Whatsapp and Telegram is offered. Also, the paper analyzes the pertinent articles of the Criminal Procedure Code and Law 19,974 in order to assess whether these bodies enable State agencies to access computer systems, infect devices with malware and use phishing techniques. Finally, brief recommendations are offered with the hope that future legal modification can adequate our legal bodies to international human rights standards.

KEYWORDS Privacy, cybersecurity, State hacking, human rights, cybercrime

Introducción

El presente artículo busca explorar los contornos normativos y el ámbito de aplicación de la regulación de medidas intrusivas, tanto en la Ley 19.974 Sobre el Sistema de Inteligencia del Estado (ley de inteligencia) como en el Código Procesal Penal. Para ello, se seguirá un análisis de las principales disposiciones que regulan la materia y cómo algunas entregan una excesiva discrecionalidad a las policías y los organismos de inteligencia, lo que merma el carácter excepcional de estas medidas y los necesarios resguardos que deben establecerse para asegurar el debido proceso y el respeto de los derechos fundamentales de imputados, sospechosos y afectados.

El trabajo está estructurado de la siguiente manera: la primera sección consiste en una breve relación de los hechos vinculados con la denominada «Operación Huracán», cuyos pormenores han sido dados a conocer por el periodismo de investigación,[1] una comisión investigadora de la Cámara de Diputados y distintos procesos judiciales. A partir de estos antecedentes, se busca por un lado dar cuenta de las deficiencias normativas que han dado pie a un uso abusivo de ciertas facultades que el ordenamiento jurídico otorga a las policías y organismos de inteligencia, pero también de las prácticas institucionales que se han generado en torno a estas atribuciones. Esta relación busca que estos antecedentes sirvan como orientación al análisis técnico y dogmático que se desarrollará en las secciones subsiguientes del escrito.

La segunda sección propone describir de forma breve —más allá de su legalidad— las herramientas y técnicas informáticas que las policías y los organismos de inteligencia podrían eventualmente utilizar a fin de obtener acceso al contenido de las comunicaciones hechas a través de sistemas informáticos. Para ello, se describe el funcionamiento y la viabilidad técnica de la interceptación de comunicaciones, el acceso informático (*hacking*), la infección de dispositivos a través de programas maliciosos (*malware*) y el *phishing* como mecanismo de habilitación de estas dos últimas técnicas.

El tercer apartado analiza en detalle las normas que permiten la ejecución de diligencias intrusivas que pueden afectar el derecho constitucional a la intimidad y la inviolabilidad de las comunicaciones privadas. Este análisis busca dilucidar si los organismos de inteligencia y las policías se encuentran habilitados para echar mano a técnicas de acceso informático o *hacking* al momento de recolectar información en el ámbito de la inteligencia o producir prueba al interior del proceso penal.[2]

1. Nicolás Sepúlveda y Mónica González, «"Operación Huracán": Testimonios y confesiones confirman que fue un montaje», *Ciper Chile*, 13 de marzo de 2018, disponible en http://bit.ly/38hdxeM.

2. A modo de prevención, es importante notar que al referirnos a acceso informático o *hacking* lo

Este análisis se concentrará en cuatro aspectos. El primero es la consagración constitucional de la inviolabilidad de las comunicaciones y la protección de la vida privada, así como la regulación de la interceptación de comunicaciones en el Código Procesal Penal. Luego, se analizará el contenido de la ley de inteligencia, con especial énfasis en los procedimientos especiales de obtención de información —en particular la intervención de comunicaciones y sistemas informáticos—, para evaluar si los verbos rectores y un análisis sistemático del cuerpo jurídico permiten concluir que los organismos de inteligencia están habilitados para llevar a cabo acciones de *hacking* en el cumplimiento de sus funciones. El tercer aspecto analizado es si la ley de inteligencia permite la utilización de técnicas que impliquen engañar al sospechoso para que entregue de manera voluntaria sus credenciales de acceso o instale un *malware* en su dispositivo, en particular a través del *phishing*. Para finalizar, se hará un análisis dogmático respecto de si la utilización de *malware* para infectar el equipo de un sospechoso cumple con el principio de proporcionalidad, o si, por el contrario, constituye una intromisión excesiva, no amparada por nuestro ordenamiento jurídico.

Por último, se ofrecen conclusiones preliminares y recomendaciones de modificación legal que buscan fortalecer nuestra legislación, con el fin de que este tipo de episodios no vuelvan a ocurrir, propender a una profesionalización de nuestras policías y un mejor resguardo de los derechos fundamentales de los sospechosos, imputados y ciudadanos.

Operación Huracán

La agenda mediática del último trimestre del año 2017 estuvo capturada por la polémica de la llamada Operación Huracán.[3] Ocho comuneros mapuches fueron deteni-

haremos desde una perspectiva técnica y no en los términos de la Ley 19.223 sobre delitos informáticos. En otras palabras, nos referimos a medidas intrusivas de carácter informático que operan superando una barrera o medida de protección.

3. Véase, por ejemplo, P. Campos y M. Alarcón, «Corte Suprema ordena liberar a comuneros detenidos por Operación Huracán», *Diario UChile*, 19 de octubre d 2017, disponible en http://bit.ly/369B9QJ; Andrés López, «Suprema ordena liberar a detenidos por Operación Huracán», *La Tercera*, 19 de octubre de 2017, disponible en http://bit.ly/2LvLEGq; «Vocero de la CAM fue detenido por supuesto vínculo con ataques incendiarios», *Cooperativa.cl*, 23 de septiembre de 2017, disponible en http://bit.ly/38iFhQy; Paula Tupper, «"Operación Huracán": Formalizarían por ley antiterrorista a los ocho detenidos», *La Nación*, 24 de septiembre de 2017, disponible en http://bit.ly/369BzGN; Victoria Viñals, «Las marcas que la "Operación Huracán" dejó en el mundo mapuche», *Diario UChile*, 24 de septiembre de 2017, disponible en http://bit.ly/2rdm6XG; Gerson Guzmán, «Operación Huracán: 6 meses de diligencias que terminaron con 8 detenidos por atentados», *Biobío Chile*, 25 de septiembre de 2017, disponible en http://bit.ly/2LxjVVw; Christian Monzón, «"Operación Huracán": Director nacional de inteligencia de Carabineros asegura que "este es el primer paso"», *Publimetro*, 24 de septiembre de 2017, disponible en http://bit.ly/38cKt8l, entre otras.

dos y acusados de asociación ilícita por supuestos lazos con la Coordinadora Arauco-Malleco. La principal evidencia aportada por Carabineros para fundar la detención de los comuneros fueron mensajes provenientes de aplicaciones de mensajería instantánea celular (Whatsapp y Telegram) supuestamente interceptados.

Estos mensajes darían cuenta del ingreso de armas de fuego desde Argentina.[4] La primera reacción de la comunidad técnica y los expertos en derecho y tecnología fue de incredulidad.[5] Después de todo, resultaba difícil creer que la policía chilena contara con la capacidad técnica de quebrar el protocolo de cifrado de Whatsapp y Telegram.[6]

En un esquema simplificado, el cifrado de punto a punto consiste en una tecnología de criptografía asimétrica que utiliza un sistema de llave pública y llave privada para asegurar la confidencialidad, autenticidad e integridad de la información a través de la aplicación de complejos algoritmos matemáticos (Granados, 2006: 12).[7] De esta forma, es posible asegurar que: i) solo el destinatario será capaz abrir y «entender» el mensaje que se ha cifrado; ii) el mensaje efectivamente proviene de quien dice haberlo enviado; y, iii) que el mensaje no ha sido modificado en tránsito o durante su almacenamiento. Esto implica que ningún tercero —distinto de los intervinientes de la comunicación— tendrá acceso a la información cifrada, ni siquiera las plataformas de comunicación (Whatsapp, Telegram, Signal, etcétera) o las compañías que proveen acceso a internet.[8]

---

4. Estos mensajes fueron filtrados a la prensa, que los reprodujo de forma íntegra el 26 de septiembre de 2017. «Mensajes atribuidos por Carabineros a mapuches detenidos dan cuenta de envío de armas desde Argentina», *El Mercurio*, 26 de septiembre de 2017, disponible en http://bit.ly/3513zfQ.

5. Al respecto, véase Daniel Álvarez Valenzuela y Cristian Bravo Lillo, «Caso Huracán: ¿es factible técnica y legalmente "hackear" Whatsapp?», *Ciper Chile*, 7 de febrero de 2018, disponible en http://bit.ly/2OWjN4c.

6. Whatsapp utiliza cifrado de punto a punto en todas sus conversaciones a partir del 5 de abril de 2016, cuando anunció la adopción del protocolo desarrollado por Open Whisper Systems —el mismo utilizado por Signal—, el cual es considerado como el más seguro en el mercado de las aplicaciones de mensajería (moxieo, «WhatsApp's Signal Protocol integration is now complete», blog de Signal, 5 de abril de 2016, disponible en http://bit.ly/2RtsCUA). Los aspectos técnicos de este sistema se encuentran descrito y disponibles públicamente en un *white paper* publicado por la empresa («Whatsapp encryption overview», sitio web de Whatsapp, 19 de diciembre de 2017, disponible en https://bit.ly/2Pknyzf). Por su parte, Telegram solo cuenta con cifrado de punto a punto en sus «conversaciones secretas», pero no en conversaciones bilaterales comunes ni en las conversaciones en grupo. Por otro lado, el cifrado de Telegram es producido por la misma empresa, lo que no es considerado una buena práctica al interior de la industria (Lee y otros, 2017). Del mismo modo, varios investigadores han sido capaces de identificar vulnerabilidades en su protocolo de cifrado («Security Analysis of Telegram», MIT Computer Science and Artificial Intelligence Laboratory, 18 de mayo de 2017, disponible en https://bit.ly/2DUzMcF).

7. Para un análisis del cifrado en nuestro ordenamiento jurídico, así como la evolución de la discusión sobre su regulación en el derecho norteamericano y europeo, véase Álvarez Valenzuela (2019b).

8. Es importante tener en cuenta que no necesariamente se tiene que romper el sistema de cifrado de

Las versiones entregadas por Carabineros fueron variadas y contradictorias. En un primer momento, se dijo que la información había sido obtenida a través de la interceptación de los mensajes de Whatsapp y Telegram, lo que por necesidad requiere de la capacidad para romper sus protocolos de cifrado. Luego, la versión cambió y se afirmó que en realidad se trataba de un *keylogger,* un programa capaz de llevar un registro de las teclas que oprime quien maneja un dispositivo y enviar este historial a un tercero. Sin embargo, esto resultaba muy improbable, ya que para reconstruir una conversación —como las que fueron publicadas en la prensa luego de la detención de los sospechosos— se tendría que haber infectado a los dispositivos de ambos intervinientes de la comunicación.

Al final, ante la falta de sustento de las versiones anteriores y sus contradicciones, Carabineros aclaró que, en realidad, el contenido de los mensajes supuestamente interceptados había sido obtenido a través de un programa malicioso (*malware*) diseñado por un funcionario de la institución. Para ello, este *malware* llamado «Antorcha» era —según la versión de la institución— introducido en los dispositivos de los sospechosos a través del envío de enlaces publicitarios falsos (*phishing*) para obtener el control de sus celulares y de esta forma acceder al contenido de las aplicaciones de mensajería antes de que los mensajes fueran cifrados. Para explicar su funcionamiento, Antorcha incluso fue puesto a prueba por su excéntrico creador, el ingeniero agrícola Alex Smith, durante un importante programa de televisión nacional. Sin embargo, la prueba no se llevó a cabo, ya que el servidor donde estaba alojado el software, en palabras del creador, «fue hackeado» durante la ejecución de la demostración.[9]

El caso también estuvo acompañado de una serie de irregularidades, como la manipulación fraudulenta de los celulares luego de haber sido incautados —lo que, en términos forenses, significó contaminar la cadena de custodia—,[10] el hecho de que Carabineros se haya opuesto físicamente al allanamiento de sus dependencias por parte de la Policía de Investigaciones,[11] y que el Fiscal a cargo de la investigación del delito de implantación fraudulenta de evidencia haya sido objeto de seguimiento y amedrentamiento por parte de miembros de Carabineros.[12]

---

un servicio de mensajería para obtener acceso al contenido de los mensajes. Otras formas de vulneración no descansan en interceptar la información mientras viaja cifrada. Por ejemplo, al comprometer el terminal o dispositivo mismo, es posible obtener acceso a los mensajes antes de que sean cifrados.

9. «¿Por qué el "Tío Emilio" está involucrado en la investigación de la Operación Huracán?», *La Hora*, 11 de junio de 2018, disponible en http://bit.ly/2YmKAtA.

10. «"Operación Huracán": Nueve carabineros son indagados por instalación de pruebas falsas», *Emol*, 27 de enero de 2018, disponible en http://bit.ly/2DSIEzF.

11. «Operación Huracán: Carabineros se opuso a allanamiento de la PDI y Fiscalía pide intervención del gobierno», *El Dínamo*, 26 de enero de 2018, disponible en http://bit.ly/2Ys3cIp.

12. Óscar Pérez Tapia, «Huracán: Fiscal de Temuco denuncia seguimientos», *La Tercera*, 1 de septiembre de 2018, disponible en http://bit.ly/2Yu6rPU.

Finalmente, y en medio de acusaciones cruzadas de engaño y traición entre Gonzalo Blu —el entonces director de Inteligencia de Carabineros— y Alex Smith, ambos funcionarios fueron dados de baja, mientras que este último admitió que el software Antorcha en realidad nunca existió,[13] y que el contenido de los informes de inteligencia de Carabineros era derechamente inventado.[14] Estas irregularidades dieron pie a la creación de una comisión investigadora de la Cámara de Diputados, cuyo informe concluyó que «la utilización de pruebas falsas u obtenidas fraudulentamente en el marco Operación Huracán fue un montaje llevado adelante por la Unidad de Inteligencia de Carabineros para incriminar a personas pertenecientes al pueblo mapuche».[15]

Al momento de la redacción de este artículo, la responsabilidad penal de los intervinientes en este episodio todavía se discute en varios procesos judiciales. Del mismo modo, a pesar de que el programa Antorcha resultó ser falso, el caso de Operación Huracán permite orientar el análisis de nuestra legislación y las prácticas institucionales de los organismos de seguridad para responder la interrogante que este artículo se propone: ¿Hasta qué punto se ajusta a nuestro ordenamiento jurídico la utilización de técnicas de *hacking* estatal en el contexto de la persecución penal y las labores de inteligencia?

¿Es técnicamente posible comprometer el contenido de las comunicaciones en aplicaciones de mensajería instantánea?

Las diligencias al interior de Operación Huracán fueron defendidas por Carabineros bajo el argumento de que se encontraban legalmente habilitadas por la ley de inteligencia. A fin de evaluar si dicho acceso informático o infección de dispositivos a través de *malware* cumplió con los requisitos establecidos en nuestro ordenamiento jurídico, será necesario dividir este análisis en dos subsecciones.

La primera consiste en una relación de las hipótesis de acceso informático que tuvieron lugar en Operación Huracán, que estará acompañada por una descripción de las acciones informáticas involucradas y otros antecedentes de carácter técnico necesarios para entender de forma correcta la relación entre las diligencias efectuadas y las figuras jurídicas que las regulan. Acto seguido —y a partir de los antecedentes

13. Mario Peñafiel Durruty, «Operación Huracán: Alex Smith admite que "Antorcha" jamás existió», *Meganoticias*, 16 de junio de 2018, disponible en http://bit.ly/2sTQYNg.

14. «PDI y Fiscalía concluyen que todos los informes de Carabineros en Op Huracán son falsos», *La Hora*, 8 de marzo de 2018, disponible en http://bit.ly/2Pz7EBt.

15. «Informe de la comisión especial investigadora de la actuación de los organismos policiales, de persecución criminal y de inteligencia en torno a la supuesta existencia de pruebas falsas en el marco de la denominada "Operación Huracán"», sitio web de Cámara de Diputados, p. 188, disponible en https://bit.ly/2PlKf6i.

anteriores—, se hará un análisis jurídico de las disposiciones de la ley de inteligencia y el Código Procesal Penal para dilucidar si los organismos de inteligencia y las policías se encuentran legalmente habilitadas para hackear dispositivos, aprovecharse de vulnerabilidades informáticas y utilizar técnicas de *phishing*.

En términos forenses, existe una multiplicidad de técnicas informáticas que los organismos de inteligencia y las policías pueden utilizar, más allá de su eventual ilegalidad.[16] A continuación, se describen de manera breve las más atingentes al caso en estudio.

Interceptación de las comunicaciones

Ya que las aplicaciones de mensajería instantánea son utilizadas en dispositivos celulares, el contenido de la comunicación es transmitido de forma inalámbrica a través de ondas electromagnéticas. Esto hace que la información sea susceptible de ser interceptada mientras viaja entre el emisor y el receptor.

Para asegurar la confidencialidad de las comunicaciones, las distintas aplicaciones han optado por utilizar protocolos de cifrado. Como resultado, aun cuando la información es interceptada, no es posible que terceros sean capaces de descifrar el contenido de la comunicación.

La primera versión de Carabineros señalaba que los mensajes de los comuneros habían sido obtenidos mediante la interceptación de sus comunicaciones a través de Whatsapp y Telegram. Como ya mencionamos, ambas aplicaciones utilizan sistemas de cifrado de punto a punto, lo que hace altamente improbable que Carabineros sea capaz de quebrar su sistema de cifrado.[17] De hecho, ni siquiera a nivel comparado

16. Así, Mayer (2018: 166-167) distingue entre delitos informáticos y las acciones o medios que los permiten: «El comportamiento de los delitos que inciden en el soporte lógico de un sistema informático e implican el uso de redes computacionales se identifica, en términos generales, con alguna de las siguientes conductas: aquellas que suponen destrucción o inutilización de datos o programas de sistemas informáticos, que suelen vincularse con el concepto de sabotaje informático; las que implican acceso u obtención indebidos de datos o programas de sistemas informáticos, que suelen ligarse con la idea de espionaje informático; y las que suponen alteración o manipulación de datos o programas de sistemas informáticos, que suelen vincularse con el concepto de fraude informático. […] Igualmente, existen comportamientos que pueden ser difíciles de encasillar en alguno de los tres grupos de hipótesis indicados *supra*, fundamentalmente porque pueden llevarse a cabo para posibilitar o facilitar la ejecución de otras conductas que integran la criminalidad informática. Es lo que ocurre, por ejemplo, con la difusión de *malware* o software malicioso, o con el acceso indebido a datos o programas informáticos —también conocido como *hacking*—, que pueden orientarse a la ejecución de un sabotaje informático, de un espionaje informático, o bien, de un fraude informático».

17. Previo a la implementación de cifrado de punto a punto, era posible acceder a las comunicaciones de Whatsapp de un tercero con el solo hecho de estar conectado a la misma red de wifi. Véase Sudhir Shukla, «How to access (hack) someone else's Whatsapp account», *Tech4more*, 9 de septiembre de 2014, disponible en http://bit.ly/2Pigsvc.

se ha comprobado que exista la capacidad técnica para quebrar estos protocolos de cifrado.[18]

Acceso informático o hacking

Para efectos de este artículo, entenderemos el acceso informático o *hacking* como «el acceso a un sistema de tratamiento de la información con el ánimo de conocer indebidamente de la información contenida en él» (Medina, 2014: 84). A nivel comparado, se ha entendido que la punibilidad de esta conducta requiere la superación de una barrera técnica (o medida de seguridad) y que la información contenida en el sistema de tratamiento se encuentre protegida contra el acceso indebido.[19]

Para lograr este acceso indebido, el atacante suele apoyarse sobre todo en dos estrategias. La primera consiste en «engañar»[20] al sistema de tratamiento de la información, haciéndose pasar por el administrador o por un usuario con mayores permisos. De esta forma, la obtención fraudulenta de las contraseñas de un usuario a través de distintas modalidades de ingeniería social puede constituir una forma de *hacking*.

La segunda modalidad corresponde a la explotación de una vulnerabilidad informática, de forma tal de obtener acceso a un sistema a pesar de que éste se encuentre —en principio— prohibido o requiera de mayores permisos que los que el atacante cuenta. En este sentido, las vulnerabilidades informáticas pueden ser definidas como «debilidades u otras condiciones en una organización que un actor externo, como un hacker, un Estado-nación, un empleado descontento u otro atacante, puede explotar para afectar negativamente la seguridad de los datos».[21]

Así, por ejemplo, un atacante puede aprovecharse de un error en el código de un programa para obtener un acceso no autorizado al sistema de información. Estas vulnerabilidades pueden haber sido parte del programa desde su creación, caso en el cual, de no haber sido reportadas y parchadas, se les denomina vulnerabilidades de

18. Álvarez Valenzuela y Bravo Lillo («Caso Huracán: ¿Es factible…») descartan esta posibilidad, por la dificultad que significa en términos de recursos y capacidad técnica alcanzar este objetivo.

19. De esta forma, Medina (2014) cita la sección 202.a del *Strafgesetzbuch* alemán, que define el espionaje de datos como «quien sin autorización se procure para sí o para otro acceso a datos que no estén destinados a él y que estén especialmente asegurados contra su acceso no autorizado, por medio de la superación de la protección de acceso, será castigado con pena privativa de libertad de hasta tres años o con multa».

20. Para una interesante discusión epistemológica respecto de la posibilidad de que una máquina sea susceptible de ser engañada, véase Muñoz (2013).

21. «Vulnerabilities are weaknesses or other conditions in an organization that a threat actor, such as a hacker, nation-state, disgruntled employee, or other attacker, can exploit to adversely affect data security» (la traducción es nuestra). Sean Atkinson, «Cybersecurity tech basics: Vulnerability management: Overview», Practical Law, 2018, disponible en https://bit.ly/2Phg4wQ.

día cero o *zero day*; tratarse de errores en el código producido por una modificación errónea por parte de su autor; o tratarse de una vulnerabilidad informática que un gobierno ha obligado a la empresa desarrolladora a incluir en su código, las que se denominan puertas traseras o *backdoors*.

En estricto rigor, sería posible obtener acceso al contenido de las aplicaciones de mensajería explotando una vulnerabilidad en su código o del sistema operativo del dispositivo. Sin embargo, los estándares de seguridad de este tipo de programas son bastante altos y la información sobre vulnerabilidades de día cero que se prestan para este propósito se transan por precios que van entre los US$ 500.000 y US$ 1 millón.[22]

Infección a través de programas maliciosos (malware)

Para efectos de este artículo, entenderemos por programa malicioso o *malware* aquel programa que fue escrito o adquirido con la finalidad de abusar o explotar una vulnerabilidad informática. Entre las categorías de *malware* podemos encontrar los virus (programas que se esconden en el código de otro para propagarse), los gusanos (programas independientes), los troyanos (programas que tienen una funcionalidad aparentemente útil, pero esconden otra funcionalidad maliciosa) y los *rootkit* (programas que tienen por objetivo apoderarse del sistema operativo completo y se esconden en sus funcionalidades básicas).

La utilización de programas maliciosos puede responder a objetivos variados, como

> la destrucción de datos alojados en servidores o computadoras personales, pasando por la mera demostración de la vulnerabilidad de los sistemas, hasta el desvío de los servidores DNS con el objeto de redirigir la navegación para la propagación de publicidad, o bien, para introducirse en sistemas de información, a través de la utilización o simulación de datos reales a fin de hacer creer a la víctima que se está contactando con un usuario real, por ejemplo, una página de una entidad bancaria por internet u otro servicio de carácter comercial (Oxman, 2013: 216).

Una de las principales diferencias entre el mero *hacking* y la utilización de programas maliciosos es que el segundo permite modificar la información contenida o sabotear el funcionamiento del sistema de tratamiento de la información. En este sentido, el programa Antorcha corresponde a un *malware*, ya que no solo permitía obtener acceso a los dispositivos, sino que supuestamente tenía la capacidad de infectar los terminales a través de un correo electrónico —sin la necesidad de que el usuario abriera el correo— y permitía la creación de un espejo del equipo infec-

22. Lorenzo Franceschi-Bicchierai, «You can now get $ 1 million for hacking Whatsapp and iMessage», *Vice Motherboard*, 7 de enero de 2019, disponible en http://bit.ly/2PqI1mb.

tado, tras lo cual enviaba una copia de las conversaciones a Carabineros (Colomés, 2018).[23]

A nivel comparado, se ha reportado la utilización de *malware* por parte del gobierno de México para espiar a activistas de derechos humanos y periodistas. Este programa se infectaba en los dispositivos de las víctimas a través de enlaces enviados por mensajes de texto y permitía a su controlador obtener acceso al contenido de las comunicaciones en distintas aplicaciones de mensajería instantánea (Pérez de Acha, 2016: 44-48). De esta forma, la utilización de un programa similar por parte de la policía chilena es en teoría posible.

Phishing

A diferencia de los casos anteriormente descritos, el *phishing* hace las veces de mecanismo de habilitación para el acceso no autorizado y la infección de dispositivos con programas maliciosos. Esta técnica puede ser definida como la pesca de datos «a través del envío masivo de correos electrónicos con enlaces a páginas web falsas, respecto de las cuales se imita el contenido o la imagen de un determinada entidad financiera o bancaria para engañar al destinatario del mensaje, logrando así sustraer la información personal que posibilita el acceso a sus cuentas» (Oxman, 2013: 2017).

Se trata de una forma de ingeniería social que —a través del engaño— consigue que la víctima entregue de manera voluntaria sus credenciales de acceso, datos personales o instale un programa malicioso en su dispositivo.

Supuestamente, el software Antorcha era implantado en los dispositivos de los sospechosos a través de correos electrónicos que se hacían pasar por avisos publicitarios. Esta situación fue reconocida por Gonzalo Blu, quien lamentó de manera pública en una entrevista que estos antecedentes salieran a la luz, ya que ponía de sobre aviso a los delincuentes que no tienen que hacer clic en los enlaces sospechosos que reciben, lo que podía dificultar la utilización de esta técnica a futuro.[24]

23. Es importante notar que puede existir una relación de medio a fin entre dichas conductas, pues mediante el uso de *malware* es posible hackear, sin perjuicio que, como ya se indicó, el uso de dicho *malware* amplía el rango de acción al poder manipular la información contenida en los sistemas informáticos a los cuales se accede.

24. Cámara de Diputados, «Informe de la comisión», p. 129.

Tipos de intervención informática eventualmente permitidos por la legislación chilena

Interceptación de comunicaciones a nivel constitucional y el Código Procesal Penal

Nuestra Carta Fundamental, en su artículo 19, numeral 5, garantiza a todas las personas «la inviolabilidad del hogar y de toda forma de comunicación privada», y agrega que «el hogar solo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley».

El requisito de contar con una habilitación expresa por parte de la ley para restringir el derecho a la inviolabilidad de las comunicaciones se refuerza por el contenido del artículo 63 de la Constitución, que establece el *dominio legal máximo*.

Lo anterior corresponde a lo que la doctrina ha denominado *principio de reserva legal* o *principio de legalidad* (Nogueira Alcalá, 2003). De esta forma, la Constitución impone que la restricción o afectación de garantías constitucional solo pueden ser establecidas mediante una ley. Por lo tanto, las fuerzas estatales solo podrán hacer uso de estas medidas cuando estén expresamente habilitadas para ello y éstas «cumplan con los estándares de especificidad y determinación y que no afecten la esencia del derecho protegido» (Álvarez Valenzuela, 2018: 20).

Dicho principio reserva al legislador un conjunto de materias, excluyendo de su esfera a otros poderes del Estado, en atención a la posible afectación o restricción de derechos fundamentales que esto podría ocasionar (Cordero, 2015: 89). En consecuencia, se ha entendido como una garantía sustantiva de los derechos fundamentales de las personas. Zapata (2000: 193) afirma que con él se busca garantizar que la ciudadanía —a través de los representantes que ha escogido— sea quien defina las regulaciones que afecten de forma directa su libertad o propiedad. En el mismo sentido, a juicio de Fermandois (2001: 288), el debilitamiento de este principio afecta de manera directa a las personas, al excluirlas de temas trascendentes para el bien común, como lo es la afectación o restricción de derechos fundamentales. Por último, y en esta misma línea, el Tribunal Constitucional ha señalado que el propósito de este mandato es hacer previsible para los eventuales afectados una apertura de sus comunicaciones.[25]

Conforme a esta exigencia constitucional, el Tribunal Constitucional ha considerado que, para que la ley autorice la interceptación de documentos o comunicaciones, se deben definir antes los casos en los que dicha autorización será posible. Además, se debe establecer el procedimiento mediante el cual se otorgará la autorización. Por último, la autorización legal debe ser determinada, por lo que no pueden establecer situaciones o casos genéricos.[26]

25. Sentencia Tribunal Constitucional, rol 2.153, 11 de septiembre de 2012, considerando 38.

26. Sentencia Tribunal Constitucional, rol 2.153, considerando 38.

Directamente relacionado con la garantía de la inviolabilidad de las comunicaciones, se encuentra aquella consagrada en el numeral 4 del artículo 19, que garantiza el «respeto y protección de la vida privada y la honra de la persona y su familia, y, asimismo, la protección de sus datos personales».

Ambas garantías se encuentran vinculadas al «constituir a su vez una estación indispensable en la vía aseguradora del respeto y protección de la vida privada de las personas, es decir su intimidad» (Zapata, 2009: 78).

En cumplimiento de su mandato constitucional, la regulación penal resguarda con igual recelo y cautela la ejecución de diligencias intrusivas que tienen el potencial de restringir o vulnerar el derecho a la inviolabilidad de las comunicaciones y la protección de la vida privada.

De esta forma, el Código Procesal Penal contiene una serie de medidas intrusivas, las que son definidas por la doctrina como «actividades de investigación o búsqueda de pruebas dentro de algún ámbito de privacidad de las personas que la ley protege, como son, por ejemplo, el domicilio, las comunicaciones privadas, el cuerpo y los vestidos de la persona, su correspondencia y otras» (Cavada, 2018: 1).[27]

Como afirman Núñez y Correa (2017: 196), lo anterior se justifica, pues no es posible imaginar la persecución penal ni el ejercicio del poder punitivo de un Estado sin entender que la operatividad de su justicia podría implicar una afectación a las garantías individuales consagradas en la Constitución.

Así, tanto los derechos y garantías fundamentales como las eventuales afectaciones no son absolutos, por lo que se requiere una adecuada ponderación entre ellos. Surge, entonces, la figura de restricción de derechos fundamentales, que corresponde a un «mecanismo de control de la constitucionalidad de las actuaciones estatales lesivas». Esta figura cumple una doble función: en primer lugar, opera como «límite de los límites» y, en segundo lugar, determina el contenido esencial de los derechos fundamentales, como consecuencia de la ponderación entre el derecho fundamental y la afectación conforme al principio de proporcionalidad (Núñez y Correa, 2017: 197-198).

En el caso del derecho procesal penal chileno, se reconocen límites formales al establecimiento de la verdad en el procedimiento, que corresponden a «garantías impuestas por el ordenamiento jurídico como límite a la persecución penal del Estado y más precisamente a la actividad probatoria desplegada por éste en el establecimiento de la verdad» (Horvitz y López, 2002: 99).

A continuación, revisaremos los artículos del Código Procesal Penal que regulan

27. Se entiende por comunicaciones privadas todo «acto comunicativo que se proyecta de una persona hacia otra (que pueden ser una o varias personas) quien ha sido escogida por el emisor y donde no importa el contenido ni el medio por el cual se materialice la comunicación» (Álvarez Valenzuela, 2019b: 253).

las medidas intrusivas dentro de la etapa investigativa desarrollada por el Ministerio Público, y que tienen el potencial de afectar las garantías de inviolabilidad de las comunicaciones y el respeto de la vida privada.

El artículo 218 del Código regula la retención e incautación de correspondencia, entendiendo por tal «la correspondencia postal, telegráfica o de otra clase y los envíos dirigidos al imputado o remitidos por él», que incluye la que se presuma que emanan de él o que éste pudiera ser su destinatario. La norma también considera de manera expresa la obtención de correspondencia electrónica dirigida o emanada del imputado. Además, exige que existan motivos fundados que justifiquen su utilidad para la investigación.

Por su parte, el artículo 219 permite que el fiscal solicite copias de las comunicaciones transmitidas o recibidas por empresas de comunicaciones, incluyendo las transmisiones de radio, televisión y otros medios.

Finalmente, el artículo 222 permite la interceptación y grabación de las comunicaciones telefónicas o de otras formas de telecomunicación siempre y cuando «existieren fundadas sospechas, basadas en hechos determinados, de que una persona hubiere cometido o participado en la preparación o comisión, o que ella prepare actualmente la comisión o participación en un hecho punible que mereciera pena de crimen, y que la investigación lo hiciere imprescindible».[28] Por lo tanto, se trata de un estándar particularmente exigente, pues requiere el cumplimiento copulativo de los siguientes requisitos para su autorización: i) sospechas fundadas de la comisión o participación en un crimen; ii) que dichas sospechas se basen en hechos determinados; y iii) que la utilización de la medida intrusiva sea imprescindible para la investigación.

Como es posible apreciar, el Código Procesal Penal establece habilitaciones que cumplen con los requisitos de especificidad y determinación, con el fin de evitar que la ejecución de diligencias intrusivas vulnere la esencia del derecho a la inviolabilidad de las comunicaciones y la protección de la vida privada.

La ejecución de todas las diligencias contenidas en las disposiciones mencionadas requiere la existencia de una autorización previa del juez de garantía, ya sea porque el artículo lo menciona expresamente o por la aplicación subsidiaria del artículo 9 del Código, el que establece que «toda actuación del procedimiento que privare al imputado o a un tercero del ejercicio de los derechos que la Constitución asegura, o lo restringiere o perturbare, requerirá de autorización judicial previa».

28. El inciso quinto del mismo artículo establece la obligación de las compañías proveedoras de servicio de internet de mantener un listado actualizado de sus rangos autorizados de direcciones IP y un registro, no inferior a un año, de los números IP de las conexiones que hagan sus abonados. Para un análisis sobre los eventuales problemas de compatibilidad entre los esquemas de retención general de metadatos o datos de tráficos y los derechos fundamentales de la población, véase Canales y Viollier (2018).

A su vez, el principio de proporcionalidad se materializa en dichos artículos a través de la exigencia de establecer de manera específica bajo qué circunstancias y modalidad es posible la utilización de las medidas reguladas. El hecho de que la interceptación de comunicaciones contenida en el artículo 222 requiera que el delito merezca pena de crimen, da cuenta de que la voluntad del legislador es reservar este tipo de diligencias intrusivas para casos de especial gravedad.

Por último, los verbos rectores y la terminología utilizada por los artículos estudiados dan cuenta que éstos permiten al Ministerio Público retener e incautar comunicaciones, solicitar copias de ellas o incluso interceptar el contenido de los mensajes. Todas estas diligencias se basan en que esta información puede ser obtenida a través de la colaboración de las empresas de comunicaciones o por ser la comunicación posible de ser interceptada mientras viaja entre el emisor y el receptor. Sin embargo, no existen elementos normativos que permitan argumentar que estas disposiciones habilitan al Ministerio Público a utilizar técnicas informáticas que le permita obtener acceso o modificar el contenido de un sistema de tratamiento de la información, sujeto a medidas técnicas de seguridad.

Intervención de sistemas y redes informáticos al alero de la ley de inteligencia

La ley de inteligencia

La ley de inteligencia tiene por objetivo regular el Sistema de Inteligencia del Estado (artículo 1). Esto es, el conjunto de organismos de inteligencia, independientes entre sí, que dirigen y ejecutan actividades específicas de inteligencia para asesorar al presidente de la República y a los diversos niveles superiores de conducción del Estado, con el objetivo de proteger la soberanía nacional y preservar el orden constitucional, y que, además, formulan apreciaciones de inteligencia útiles para la consecución de los objetivos nacionales (artículo 2).

Para la consecución de este objetivo —y como consta en la historia de la ley—, este cuerpo jurídico regula «la utilización de técnicas intrusivas y métodos encubiertos definidas como los procedimientos que —en base a la simulación, la disimulación, la observación o la tecnología— permitan acceder a información contenida en fuentes cerradas».[29]

Para la utilización de estas medidas intrusivas, se establece de forma expresa la necesidad de autorización judicial previa; los directores de los organismos de inteligencia —en persona o a través de algún funcionario expresamente designado al efecto— deberán solicitar la señalada autorización al ministro de la Corte de

29. «Historia de la Ley 19.974», Biblioteca del Congreso Nacional, p. 9, disponible en https://bit.ly/2qvyOk5.

Apelaciones en cuyo territorio se llevará a cabo la diligencia o donde ésta se inicie (artículo 25).[30]

Dicha autorización debe cumplir con los siguientes requisitos generales: i) debe dictarse sin audiencia ni intervención del afectado o tercero; ii) debe ser fundada; y iii) debe incluir la especificación de los medios que se emplearán, la individualización de la o las personas a quienes se le aplicará la medida y el plazo de la medida, el cual no puede ser superior a 90 días, prorrogable una única vez por igual plazo. Que la autorización judicial requiera pronunciarse sobre los medios utilizados da cuenta del necesario análisis de proporcionalidad que la legislación exige que el juez desarrolle. Así, una autorización que no se pronuncie específicamente sobre los mecanismos para obtener la información no cumpliría este estándar de proporcionalidad.

Según lo dispuesto en el artículo 23, la utilización de estas medidas intrusivas requiere que la información que se pretende obtener sea estrictamente indispensable para cumplir los objetivos del Sistema de Inteligencia y que no puedan obtenerse desde fuentes abiertas. Además, la ley establece que dichos procedimientos están limitados a las actividades de inteligencia[31] y contrainteligencia,[32] cuyo objetivo es resguardar la seguridad nacional y proteger al país del terrorismo, crimen organizado y narcotráfico (artículo 23).

Procedimientos especiales de obtención de información

La ley define los procedimientos especiales de obtención de información como aquellos que «permiten el acceso a antecedentes relevantes contenidos en fuentes cerradas o que provienen de ellas, que aporten antecedentes necesarios al cumplimiento de la misión específica de cada organismo operativo» (artículo 24).

El mismo artículo enumera cuatro procedimientos especiales de obtención de información. El primero, regulado en la letra a) del artículo 24, permite "la intervención de las comunicaciones telefónicas, informáticas, radiales y de la correspondencia en cualquiera de sus formas». La letra b) del mismo artículo permite «la intervención de sistemas y redes informáticos».

30. Esta regulación responde al principio de autorización judicial previa, el cual, según lo señalado en el mensaje presidencial de la ley, es un resguardo efectivo de los derechos de las personas, más aún si se tiene en cuenta que tal autorización solo será procedente ante fundadas sospechas de amenaza grave para la seguridad de personas, autoridades o instituciones, o de la seguridad pública («Historia de la Ley», p. 11).

31. Entendiéndose por tales el proceso sistemático de recolección, evaluación y análisis de información, cuya finalidad es producir conocimiento útil para la toma de decisiones (artículo 2, letra a).

32. Definida como aquella parte de la actividad de inteligencia cuya finalidad es detectar, localizar y neutralizar las acciones de inteligencia desarrolladas por otros Estados o por personas, organizaciones o grupos extranjeros, o por sus agentes locales, dirigidas contra la seguridad del Estado y la defensa nacional (artículo 2, letra b).

Por su parte, la letra c) autoriza la «escucha y grabación electrónica incluyendo la audiovisual» y, finalmente, la letra d) permite la «intervención de cualesquiera otros sistemas tecnológicos destinados a la transmisión, almacenamiento o procesamiento de comunicaciones o información».

La primera diferencia entre la regulación de las medidas intrusivas contenidas en el Código Procesal Penal y la ley de inteligencia es la utilización de verbos rectores distintos; mientras el primer cuerpo legal utiliza el vocablo *interceptación* de comunicaciones, el segundo habla de *intervención*. Esto es relevante, puesto que la elección de verbos rectores distintos da cuenta de que el legislador buscó habilitar a los organismos de inteligencia para llevar a cabo medidas más intrusivas que aquellas permitidas al interior del proceso penal.

En cuanto a la terminología, la palabra *interceptar* evoca la noción de detener una cosa o apoderarse de ella antes de que llegue a destino. Es posible argumentar que la utilización del término *interceptar* necesariamente se refiere al hecho de atajar, obtener acceso, copia fidedigna o retener el contenido de la comunicación mientras ésta se encuentra viajando entre el emisor y el receptor, ya sea a través de ondas electromagnéticas o cables de transmisión. Sería imposible, por tanto, interceptar información que se encuentra almacenada, por ejemplo, en un servidor o sistema informático, toda vez que ésta no se encuentra en tránsito.

Por el contrario, el término *intervenir* evoca la idea de tomar parte en un asunto, modificar un proceso u objeto e incluso el ejercer autoridad sobre otro. En atención a lo anterior, es seguro aseverar que la habilitación contemplada en las letras a), b) y d) del artículo 24 de la ley de inteligencia contienen una habilitación más amplia que la mera interceptación de comunicaciones.[33]

Esta constatación se ve reforzada por el hecho de que el objeto de la intervención no es solo la comunicación en cualquiera de sus soportes (letra a), sino que también los sistemas informáticos (letras b y d), lo que corresponde a una definición vaga del objeto de la intervención. Del mismo modo, la letra d) del artículo 24 adolece de una importante falta de determinación y especificidad, al permitir de forma genérica la intervención de cualquier otro sistema tecnológico. Por último, vale la pena mencionar que la letra d) hace referencia específica a la posibilidad de intervenir sistemas tecnológicos que almacenan información o comunicaciones.

Parece evidente que —hasta cierto punto— la ley habilita a los organismos de inteligencia a acceder a sistemas informáticos eludiendo barreras técnicas de seguridad, o en otras palabras, utilizar técnicas de *hacking*. Sin embargo, esta habilitación

33. Si bien la Real Academia Española define intervenir como «espiar, por mandato o autorización legal, una comunicación privada», dicho sentido solo es presentado en la quinta acepción otorgada al verbo. Por otro lado, nos parece que una interpretación armónica del cuerpo legal da a entender que el legislador utiliza el verbo intervenir en términos más amplios que solo interceptar.

no puede ser interpretada como absoluta y es necesario hacer un análisis técnico-jurídico para determinar qué herramientas y conductas informáticas se encuentran amparadas por los procedimientos especiales de obtención de información, y cuáles no pueden entenderse comprendidos, por resultar desproporcionados o por generar una afectación excesiva de los derechos fundamentales de los individuos.[34]

En este mismo sentido, el Tribunal Constitucional, en su sentencia rol 2153-11, considerando 40, señaló que

> el modelo diseñado por el legislador para interceptar, abrir o registrar las comunicaciones privadas y los documentos asociados a ellas, es coincidente con los estándares diseñados por esta Magistratura, que ha exigido habilitaciones restrictivas (STC 389/2003), con parámetros objetivos y precisos, no discrecionales (STC 198/95, 1894/2011), sujetas a control (STC 389/2003, 433/2005) y en que el afectado no padezca detrimentos excesivos (STC 1365/2009).

Para facilitar un análisis que nos permita distinguir qué herramientas y conductas resultan lícitas al amparo de la ley de inteligencia, vamos a retomar las categorías descritas en tercera sección y contrastaremos su implementación con los requisitos establecidos por el Tribunal Constitucional.

En cuanto a la interceptación de comunicaciones, parece claro que ésta se encuentra recogida entre los procedimientos especiales de obtención de información. Por un lado, porque la letra c) autoriza en forma explícita la escucha y grabación electrónica, aunque los términos ocupados no son particularmente claros. Del mismo modo, cabe argumentar que la facultad de interceptar comunicaciones queda subsumida en la de intervenir comunicaciones telefónicas, informáticas, radiales y otras formas de correspondencia (letra a), toda vez que —según el aforismo jurídico— quien puede lo más, puede lo menos.[35]

En cambio, resulta más complejo determinar qué modalidades de acceso informático o *hacking* estarían permitidos por la ley. Para ello, resulta necesario distinguir entre distintas formas de obtener este acceso indebido. Si el acceso no autorizado se configura a través de la obtención de las credenciales del afectado utilizando la técnica del *phishing*, a nuestro juicio el organismo de inteligencia estaría incurriendo en una ilegalidad, puesto que el *phishing* necesariamente requiere engañar al afectado.[36]

---

34. La doctrina ha descrito los requisitos de procedencia de estas medidas como exiguos y particularmente ambiguos, lo que permite niveles de discrecionalidad administrativa que incluso hacen dudar de su constitucionalidad (Álvarez Valenzuela, 2019a: 93)

35. Sin embargo, en términos prácticos esta facultad tenderá a perder vigencia con el paso del tiempo, toda vez que la implementación del cifrado de punto a punto se está transformando de manera sostenida en un estándar por defecto en la industria de las comunicaciones digitales.

36. Resulta decidor que el mismo Alex Smith haya reconocido el uso de esta técnica y dado a entender que Carabineros considera que la ley de inteligencia ampara la utilización del *phishing*. De esta forma, el

Las razones que justifican esta posición se desarrollan con mayor profundidad en la siguiente sección.

Por otro lado, bajo ciertas circunstancias, hay hipótesis de *hacking* que podrían entenderse amparadas por los numerales a) y d) del artículo 24. Si, por ejemplo, a través de sus herramientas forenses, un organismo de inteligencia es capaz de identificar y explotar una vulnerabilidad informática de un programa o sistema operativo del dispositivo que se busca comprometer, el acceso informático obtenido a través de esta vía podría considerarse amparado por la ley de inteligencia. Esta vulnerabilidad puede tomar la forma de un *zero-day,* una puerta trasera o un error en el código. En este caso, la intervención del sistema se configura a través del aprovechamiento de una vulnerabilidad que le permite al organismo eludir una barrera técnica de seguridad y acceder a la información contenida en el dispositivo.

La forma en que se interviene un sistema informático también puede tomar formas menos sofisticadas.[37] Por ejemplo, se podría utilizar un programa especializado para hacer un ataque de fuerza bruta (*brute force)*, el que consiste en ingresar de forma automatizada un número indeterminado de contraseñas aleatorias usando todas las combinaciones posibles hasta acertar a la correcta (Ayankoya y Ohwo, 2019: 8). Si el afectado utiliza una contraseña particularmente poco segura o común, esto puede garantizar el éxito del ataque.

Las policías también pueden registrar fuentes de acceso público en búsqueda de antecedentes que les permitan obtener las credenciales de acceso del sospechoso. De esta forma, pueden revisar los distintos repositorios de nombres de usuario y contraseñas que se encuentran a la venta en el ciberespacio y que se han recopilado con ocasión de filtraciones de bases de datos de distintos servicios en línea.[38] Si el sospechoso comparte contraseña con algunos de los servicios que ha sufrido una filtración, esto permitiría al atacante obtener acceso a su cuenta (Jaeger y otros, 2016).

Por último, la utilización de programas maliciosos o *malware* como forma de obtener acceso al sistema informático debe entenderse como no cubierto por la habilitación contenida en el artículo 24 de la ley de inteligencia. Los argumentos que apoyan esta posición serán desarrollados más adelante, cuando abordemos el cumplimiento del principio de proporcionalidad en la utilización de medidas intrusivas.

---

profesional declaró en una entrevista que «nació la necesidad de intervenir redes sociales. Lo más fácil para mí era el *phishing*. Comenté que se podía hacer y pregunté si era legal, me dijeron que por una ley, la de inteligencia, sí. Como era legal, empezamos a enviar *phishing* a distintos blancos» (Garay y Rogoff, 2018: 9).

37. De hecho, la mayoría de los ataques informáticos a nivel mundial son de carácter semántico, es decir, no atacan al sistema de información o el código, sino que buscan obtener acceso a él o datos de valor a través de las personas que los administran.

38. Para más información sobre las filtraciones de contraseñas en línea, véase «FAQs», Have I Been Pwned?, disponible en https://haveibeenpwned.com/FAQs.

El engaño como herramienta para acceder a datos

Un tercer análisis relevante respecto de las acciones informáticas que el Estado podría utilizar con el objeto de obtener información tiene relación con la posibilidad de obtener acceso a un sistema informático mediante el engaño. Para ello, analizaremos si es posible que los organismos de inteligencia utilicen la técnica del *phishing*.

Como ya revisamos, el *phishing* es un mecanismo que habilita al atacante para obtener información relevante o infectar el terminal de la víctima y que necesariamente requiere del engaño o fraude (Moscoso, 2014: 64). De esta forma, el atacante hace creer a la víctima que está entregando su información de manera voluntaria para fines legítimos. El atacante también puede inducir a la víctima al error respecto de la naturaleza del programa que instalarán en su computador o dispositivo —que es en realidad un *malware*—. Una vez instalado, el atacante es capaz de obtener acceso e incluso control sobre el sistema informático en cuestión.

En el caso de Operación Huracán, descartamos la posibilidad de que los organismos de inteligencia hayan obtenido acceso al contenido de las comunicaciones a través de la obtención del nombre de usuario y las contraseñas de los afectados. Incluso contando con dichas credenciales, no es posible obtener acceso al contenido de los mensajes de Whatsapp, a pesar de que éstos se encuentren respaldados en Google Drive de forma no cifrada.[39]

De haber en realidad existido una obtención de los mensajes de los imputados, éstos tendrían que haber sido adquiridos a través de la infección de sus dispositivos por medio de un *malware*. Sin embargo, un análisis jurídico de las disposiciones de la ley de inteligencia da cuenta de que los organismos de inteligencia no se encuentran habilitados legalmente para engañar a los sospechosos para que éstos instalen de forma voluntaria un programa malicioso en sus dispositivos.

Incluso considerando que el artículo 24 letra b) de la ley de inteligencia permite la intervención de sistemas informáticos, el *phishing*, como hemos visto, necesariamente implica utilizar «ingeniería social» con el fin de engañar al afectado.

Una revisión sistémica de nuestro ordenamiento jurídico —en particular, de las conductas que como sociedad consideramos más lesivas— permite concluir que el actuar bajo engaño como medida intrusiva se encuentra regulado de forma celosa y su interpretación debe hacerse siguiendo un criterio restrictivo.[40]

39. Para una demostración de cómo operaría este procedimiento, véase «Replicando el funcionamiento de "Antorcha" con herramientas públicamente disponibles», blog */home/chgonzalez*, 13 de febrero de 2018, disponible en http://bit.ly/36ePOdz.

40. Este especial recelo del legislador se observa no solo respecto de la regulación de medidas intrusivas, sino también respecto de los delitos o crímenes cometidos bajo engaño o ardid, que considera como un agravante de responsabilidad conforme con el artículo 12, números 1 y 5 del Código Procesal Penal. Así, en el primero se considera un agravante de la conducta típica que el ofensor haya actuado con ale-

Por su parte, el principio de reserva legal establece que las medidas intrusivas solo pueden ser hechas en la forma y condiciones específicamente establecidas por la ley. De acuerdo con el artículo 24 citado, no existen elementos normativos que permitan inferir el otorgamiento de esta facultad de engañar a los organismos inteligencia. Lo anterior, pues la autorización es exclusiva para la intervención en comunicaciones o en los sistemas y redes informáticas. Las acciones antes descritas no contemplan —ni explícita ni implícitamente— la utilización del engaño como medio para obtener acceso a tales sistemas.

A contrario sensu, nuestro ordenamiento contempla —en casos específicos y excepcionales— la existencia de medidas intrusivas que expresamente regulan la posibilidad de engañar al sospechoso para asegurar el éxito de la medida.

Así, por ejemplo, las medidas de agente encubierto o agente revelador reguladas en el artículo 25 de la Ley 20.000 que sanciona el tráfico ilícito de estupefacientes y sustancias psicotrópicas. En particular, estas medidas permiten, por una parte, que el Ministerio Público autorice a los funcionarios policiales para que se desempeñen como agentes encubiertos, es decir, que oculten su identidad oficial y se involucren o introduzcan en las organizaciones criminales con el objetivo de identificar los participantes, reunir información y recoger los antecedentes necesarios para la investigación. También se permite que el agente encubierto tenga una «historia ficticia», ordenando al Servicio de Registro Civil e Identificación a que otorgue los medios necesarios para la materialización de dicha historia. Por otra parte, un agente revelador es un funcionario policial autorizado por el Ministerio Público para simular la compra de droga con el propósito de lograr su manifestación o incautación. Así, la legislación establece de manera estricta los fines de tales medidas intrusivas, además de autorizar de forma expresa la generación del ardid para obtener la información requerida por el Ministerio Público.[41]

Esta exigencia de una habilitación especial y expresa para obtener información mediante el engaño resulta clara al constatar que la misma ley de inteligencia contempla una medida intrusiva que autoriza el engaño en su artículo 31. Éste permite que los directores o jefes de los organismos de inteligencia puedan disponer que uno de sus funcionarios, en el ejercicio de las actividades indicadas en el artículo 23, oculte su identidad con el fin de obtener información o recabar antecedentes, para lo cual

---

vosía, que entiende como actuar por traición o sobre seguro, mientras que el segundo considera como agravante de la responsabilidad penal en los delitos contra las personas el emplear fraude o disfraz.

41. Cabe destacar que en un principio la Ley 19.336, que introdujo la figura de agente encubierto en nuestra legislación, no tenía referencia alguna respecto del ámbito de actuación de los agentes encubiertos. Lo anterior intentó ser resuelto por la Ley 20.000, pues disponía que un reglamento regularía los límites y características de dichas conductas. Sin embargo, tal frase fue declarada inconstitucional por el Tribunal Constitucional, pues a su juicio estos elementos deberían estar regulados en la Ley Orgánica Constitucional del Ministerio Público (Ivelic, 2014: 153-154).

puede introducirse en organizaciones sospechosas de actividades criminales.[42] De manera expresa, se faculta el uso de agentes encubiertos y todos aquellos actos relativos a la emisión, porte y uso de la documentación destinada a respaldar la identidad creada para ocultar la del agente.

En conclusión, la exigencia de habilitación legal estricta para las medidas que afectan derechos fundamentales, sumado al principio de legalidad consagrado en la Constitución, cierra cualquier posibilidad que los organismos de inteligencia utilicen el *phishing* como mecanismo para obtener información desde fuentes cerradas.

Principio de proporcionalidad y contenido esencial de los derechos fundamentales en la utilización de programas maliciosos como forma de obtención de información

La relación entre las medidas intrusivas habilitadas por la ley de inteligencia y el principio de proporcionalidad resulta relevante, ya que —como veremos— las técnicas que pueden ser utilizadas para la intervención de dispositivos han alcanzado un nivel que permite no solo asirse del contenido de la comunicación entre los involucrados, sino también de las fotos, eventos de agenda, ubicación, gustos, lugares visitados, alimentación y hábitos de ejercicio y, en general, de todos aquellos datos que un celular inteligente administra. Se trata, en definitiva, de un control total sobre la intimidad de una persona y, eventualmente, de todos los contactos asociados a ella. Es más, tal análisis adquiere especial importancia en el caso de la utilización de programas maliciosos cuyos objetivos pueden considerar desde la obtención de la información hasta destrucción de datos o su manipulación.

El principio de proporcionalidad ha sido definido por la doctrina como un «instrumento destinado a medir si la intervención estatal es o no lícita. Y no lo será, si en la práctica ella se traduce en la anulación o derogación del derecho o libertad de que se trate» (Arnold, Martínez y Zúñiga, 2012: 86). En el mismo sentido, los autores consideran que este principio se «encuentra subsumido en el ordenamiento constitucional chileno en la garantía genérica de los derechos establecida constitucionalmente en las bases de la Institucionalidad que dan forma al Estado de derecho (artículos 6 y 7), en el principio de prohibición de conductas arbitrarias (artículo 19 numeral 2) y en la garantía normativa del contenido esencial de los derechos (artículo 19 numeral 26 de la Constitución), además del valor justicia inherente al derecho» (Arnold, Martínez y Zúñiga, 2012: 87). Es especialmente relevante para nuestro análisis la revisión

42. Resulta interesante destacar que el uso de un agente encubierto conforme a la ley de inteligencia se permite sin necesidad de autorización judicial previa, lo que muestra una regulación completamente distinta a aquella relacionada con los mecanismos especiales de obtención de información, que sí requieren de una orden judicial. Esto resulta sin duda cuestionable, atendida la eventual afectación de derechos fundamentales.

de la afectación del contenido esencial del derecho a la intimidad y la inviolabilidad de las comunicaciones.

En esta misma línea, Nogueira sostiene que «el legislador está obligado a respetar y tiene prohibido constitucionalmente afectar el contenido esencial de los derechos [lo que] constituye un límite al poder de limitar los derechos, constituyendo la dimensión constitucional del derecho proveniente de la tradición jurídica que se debe preservar» (Nogueira Alcalá, 2005: 47). Sobre la determinación del contenido esencial del derecho, el autor afirma que este corresponde a un «concepto jurídico indeterminado», el que debe ser establecido caso a caso por el Tribunal Constitucional.

Por su parte, el Tribunal ha sostenido que se afecta un derecho en su esencia cuando se lo «prive de aquello que le es consustancial, de manera tal que deja de ser reconocible y que se impide "el libre ejercicio" en aquellos casos en que el legislador lo somete a exigencias que lo hacen irrealizable, lo entraban más allá de lo razonable o lo privan de tutela jurídica».[43]

Resulta relevante revisar el rango y la naturaleza de la información a la que podrían tener acceso los organismos de inteligencia una vez infectado un dispositivo. Lo anterior es posible de constatar en relación con el caso del *malware* Remote Control System (RCS), conocido también como Pegasus, Galileo o DaVinci de Hacking Team, el cual correspondía a un software espía que era vendido a organizaciones gubernamentales. Respecto de dicho programa, Pérez de Acha (2016: 13) reportó que, una vez infectado el dispositivo, el software entregaba acceso a los

> 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, capturas de pantalla y sitios de internet visitados.

En vista de que cada día una parte más significativa de nuestras interacciones y comunicaciones privadas pasan por nuestros dispositivos electrónicos, una medida intrusiva de estas características entregaría un acceso casi absoluto a los aspectos más íntimos de la vida privada del afectado, lo que desvirtuaría las garantías fundamentales consagradas en la Constitución. Las autorizaciones de las medidas intrusivas reguladas en la ley de inteligencia son otorgadas en el marco de la inviolabilidad de las comunicaciones y del expreso mandato al legislador de regular la afectación de tal garantía. Sin embargo, como revisamos, dicha restricción es posible solo cuando el derecho fundamental no se vea afectado en su esencia.

En tal caso, siguiendo la definición propuesta por el Tribunal Constitucional y

43. Sentencia Tribunal Constitucional, rol 43-1987, considerandos 20 y 21. Así también en las sentencias del Tribunal Constitucional, roles 200, 226 y 280 (Nogueira Alcalá, 2005: 53).

teniendo en cuenta el nivel y cantidad de información al que podría acceder un *malware* al estilo de RCS o el pretendido programa Antorcha, resulta evidente que el derecho a la intimidad y la inviolabilidad de las comunicaciones se ven por completo diluidos, por lo que es imposible su ejercicio no solo por parte de sus afectados directos, sino respecto de todos aquellos contactos indirectos cuya información también ha sido obtenida mediante tales programas.

Además, una medida que permita la utilización de tal información resultaría en exceso intrusiva y desproporcionada, además de no cumplir con los requisitos establecidos por el Tribunal Constitucional respecto de que la recolección de la información debiese responder a parámetros objetivos, precisos y no discrecionales, sujetos a control y en que el afectado no padezca detrimentos excesivos, según lo ya revisado.

Sin embargo, la redacción de la ley de inteligencia no responde a tales parámetros, ya que es evidente la vaguedad en la regulación de las medidas intrusivas, sobre todo en la medida regulada en la letra d) del artículo 24, la que autoriza la intervención de «cualesquiera otros sistemas tecnológicos destinados a la transmisión, almacenamiento o procesamiento de comunicaciones o información». Como se observa, no existe determinación o límite ni respecto de la acción de intervención —salvo lo ya señalado respecto del engaño—, ni tampoco respecto del tipo de información que se pretende obtener, pues la misma medida establece de forma amplia que puede tratarse de sistemas tecnológicos relacionados con comunicaciones o información. Al no establecerse límites claros respecto del objeto de esta medida, el artículo puede ser interpretado de forma tal que dé pie a situaciones abusivas.

Desde otra perspectiva, se observa un segundo problema respecto de la utilización del *malware* para obtener información, puesto que éste permite no solo acceder y conocer la información contenida en los dispositivos afectados, sino que también modificarlos. Esto, incluso en el supuesto de que la utilización del *malware* estuviere habilitada de manera legal, entregaría a los organismos de inteligencia una potestad fácilmente abusable. Al mismo tiempo, esta facultad de modificar el contenido del dispositivo que se compromete genera un importante problema respecto de la mantención de la cadena de custodia de la evidencia digital (Arellano y Castañeda, 2012).

Cabe destacar que la preocupación anterior es resultado no solo de un análisis abstracto, sino que responde a una situación que se verificó a propósito de la Operación Huracán, en la cual se observó que los documentos que contenían las supuestas conversaciones que habrían sido obtenidas por los organismos de inteligencia se encontraban en un formato editable y habían sido manipuladas.[44]

Asimismo, la práctica sostenida del Ministerio Público de incorporar informes de la ley de inteligencia como prueba al interior del proceso penal profundiza la posibilidad de que esta facultad sea abusada. Las medidas intrusivas reguladas en la ley

44. Cámara de Diputados, «Informe de la comisión», p. 130.

de inteligencia son sustantivamente más intrusivas que las reguladas en el Código Procesal Penal, pues responden a fines diversos y permiten a Carabineros producir prueba sin la necesaria supervisión del Ministerio Público.[45]

En definitiva, la utilización de *malware* de vigilancia resulta desproporcionada e inconstitucional, tanto por el volumen como la naturaleza en extremo sensible de la información del afectado que podría ponerse a disposición de los organismos de inteligencia. Este nivel de intrusión vuelve ilusoria cualquier pretensión de privacidad por parte del afectado, quien ha visto la totalidad de su vida íntima comprometida, al punto de que el contenido de sus dispositivos puede ser modificado a distancia. De esta forma, el artículo 24 de la ley de inteligencia no cumple con los elementos mínimos exigidos para una ley que restringe o limita el ejercicio de un derecho fundamental. Esta deficiencia se vuelve palpable al constatar la vaguedad y arbitrariedad que se observa en las letras b) y d), que no cumplen con los estándares de especificidad y determinación requeridos para la habilitación legal de afectaciones a los derechos fundamentales (Álvarez Valenzuela, 2018: 20).

Conclusiones

El principio de reserva legal establece la necesidad que cualquier tipo de restricción de derechos fundamentales, como la inviolabilidad de las comunicaciones y el derecho a la intimidad, requiera la existencia de una habilitación legal expresa. Esta habilitación debe, además, ser restringida, contener parámetros objetivos y precisos, no ser discrecional, estar sujeta a control y no implicar que el afectado padezca detrimentos excesivos.

Los hechos ocurridos con ocasión de la Operación Huracán han dado pie a una interesante discusión pública sobre si los organismos de inteligencia se encuentran facultados para llevar a cabo acciones informáticas como el *hacking* y el *phishing*. Del mismo modo, la supuesta existencia del software Antorcha levantó las alertas respecto de la eventual inconstitucionalidad de la utilización de *malware* de vigilancia por parte de las policías y organismos de inteligencia.

Un análisis de estas acciones informáticas, en relación con la regulación contenida en el Código Procesal Penal y la ley de inteligencia, nos permite concluir que las medidas intrusivas contempladas en el Código no permiten la utilización de las acciones informáticas antes señaladas.

La ley inteligencia, por su parte, adolece de descripciones vagas de las medidas intrusivas autorizadas que, eventualmente, permitirían a los organismos de inteligen-

45. Una reflexión sobre cómo esta situación puede infringir el principio de no deliberación de las policías puede encontrarse en Pablo Viollier, «Cómo el gobierno de Chile ha dado rienda suelta a sus policías», Derechos Digitales, 1 de febrero de 2018, disponible en http://bit.ly/2s5fSJg.

cia utilizar vulnerabilidades de los sistemas informáticos para poder intervenirlos y obtener información de fuentes cerradas. Sin embargo, descartamos que exista una habilitación legal para la utilización del *phishing*, pues a pesar de la poca especificidad de la ley de inteligencia, ésta no autoriza el uso del engaño, elemento que resulta esencial para la utilización de esta medida.

Asimismo, el estudio de la legislación nos permite concluir que la utilización de *malware* de vigilancia no se encuentra amparada en las normas de la ley de inteligencia. En particular, por la evidente desproporción en la afectación de la esencia del derecho a la intimidad que la utilización de una herramienta de estas características implicaría.

El estudio de las disposiciones que regulan los procedimientos especiales de obtención de información en la ley de inteligencia da cuenta que éstos no cumplen con los estándares de determinación y especificidad que el Tribunal Constitucional ha exigido. De esta forma, estos preceptos pueden dar pie a interpretaciones y prácticas institucionales que, como se hizo evidente en el caso de Operación Huracán, se pueden prestar para la vulneración de los derechos fundamentales de los ciudadanos, el debilitamiento del Estado de derecho y el deterioro del profesionalismo de los organismos de inteligencia.

Atendida la gravedad de los antecedentes expuestos —y en línea con las conclusiones de la comisión investigadora de la Cámara de Diputados—, resulta necesaria una revisión profunda del artículo 24 de la ley de inteligencia. Esta revisión debe tener como objetivo que las medidas intrusivas se establezcan de forma específica y determinada, detallando el tipo de información, así como la modalidad y condiciones de acceso que podrán incurrir organismos de inteligencia al momento de llevar a cabo una diligencia de intervención de sistemas informáticos.

La habilitación para el acceso informático deberá responder criterios objetivos de necesidad y proporcionalidad, para así asegurar que este tipo de medidas sean utilizadas de forma excepcional y a través del mecanismo menos intrusivo posible.

Las condiciones bajo las cuales la Corte de Apelaciones autoriza este tipo de diligencias también merecen ser revisadas, a fin de asegurar que en los casos en que se autoriza una intervención de sistemas informáticos, exista un análisis de mérito sustancial y no solo formal. Del mismo modo, la autorización de estas medidas debe encontrarse sujeta a una evaluación judicial posterior, como mecanismo de transparencia y rendición de cuentas sobre el uso de esta herramienta, además de la elaboración de auditorías independientes y la publicación de estadísticas de forma periódica.[46]

Por último, resulta imprescindible que una futura modificación legislativa establezca una prohibición expresa de la modificación, alteración o introducción de información en el sistema con ocasión de un procedimiento de intervención informá-

46. «Hacking necessary safeguards», Privacy International, disponible en http://bit.ly/2P03NOM.

tico. De manera excepcional, una acción de estas características podría autorizarse en el caso específico de que la alteración sea necesaria para acceder al dispositivo. En este caso, se debe establecer la necesidad de dejar constancia explícita de este hecho, de forma tal que preservar la trazabilidad e integridad de la cadena de custodia digital.

Referencias

Álvarez Valenzuela, Daniel (2018). «Privacidad en línea en la jurisprudencia constitucional chilena». *Revista de Derecho Público*, 89: 11-32. DOI: 10.5354/0719-5249.2018.52027.

—. (2019a). *La inviolabilidad de las comunicaciones privadas electrónicas*. Santiago: Lom.

—. (2019b). «Algunos aspectos jurídicos del cifrado de comunicaciones». *Derecho PUCP*, 83: 241-262. DOI: 10.18800/derechopucp.201902.008.

Arellano, Enrique y Carlos Castañeda (2012). «La cadena de custodia informático-forense». *Activa*, 3 (1): 67-81. Disponible en http://bit.ly/38jjPKU.

Arnold, Rainer, José Martínez y Francisco Zúñiga (2012). «El principio de proporcionalidad en la jurisprudencia del Tribunal Constitucional». *Estudios Constitucionales*, 10 (1): 65 - 116. DOI: 10.4067/S0718-52002012000100003.

Ayankoya, Folasade y Blaise Ohwo (2019). «Brute-force attack prevention in cloud computing using one-time password and cryptographic hash function». *International Journal of Computer Science and Information Security*, 17 (2): 7-19. Disponible en http://bit.ly/2RujmzD.

Canales, María Paz y Pablo Viollier (2018). «La compatibilidad de la retención general de metadatos y el respeto a los derechos fundamentales: El caso del decreto espía». *Anuario de Derecho Público de la Universidad Diego Portales*, (2018): 155-171. Disponible en https://bit.ly/36hQU8t.

Cavada, Juan Pablo (2018). «Regulación de las medidas intrusivas». Departamento de estudios de la Biblioteca del Congreso Nacional. Disponible en https://bit.ly/2qvftiR.

Colomés, Paulo (2018). «Imprecisiones técnicas de la Operación Huracán». Presentación para la Cámara de Diputados de Chile. Disponible en https://bit.ly/2s9hrWs.

Cordero, Luis (2015). *Lecciones de derecho administrativo*. Santiago: Thomson Reuters.

Fermandois, Arturo (2001). «La reserva legal: Una garantía sustantiva que desaparece». *Revista Chilena de Derecho*, 28 (2): 287-298.

Garay, Vladimir y Zak Rogoff (2018). *Tecnología y vigilancia en la Operación Huracán: Una revisión del trabajo periodístico realizado en torno al caso*. Santiago: Derechos Digitales. Disponible en https://bit.ly/2Pmr5gt.

Granados, Gibrán (2006). «Introducción a la criptografía». *Revista Digital Universitaria*, 7 (7): 3-17. Disponible en https://bit.ly/2Po7tQA.

Horvitz, María Inés y Julián López (2002). *Derecho procesal penal chileno*. Tomo 1. Santiago: Jurídica de Chile.

Ivelic, Armando (2014). «El agente encubierto en los delitos de tráfico ilícito de estupefacientes». *Revista Jurídica del Ministerio Público*, 61: 147-166. Disponible en https://bit.ly/340doL4.

Jaeger, David, Chris Pelchen, Hendrick Graupner, Feng Cheng y Christoph Meinel (2016). «Analysis of publicly leaked credentials and the long story of password (re-)use». Hasso Plattner Institute, Universidad de Potsdam. Disponible en https://bit.ly/2E7ZTo1.

Lee, Jeeun, Rakyong Choi, Sungsook Kim y Kwangjo Kim (2017). «Security analysis of end-to-end encryption in Telegram». Simposio en Criptografía Seguridad Informática, Naha, Japón. Disponible en https://bit.ly/36aX3TK.

Mayer, Laura (2018). «Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos». *Ius et Praxis,* 24 (1): 159-206. DOI: 10.4067/S0718-00122018000100159.

Medina, Gonzalo (2014). «Estructura típica del delito de intromisión informática». *Revista Chilena de Derecho y Tecnología*, 3 (1): 79-99. DOI: 10.5354/0719-2584.2014.32221.

Moscoso, Romina (2014). «La Ley 19.223 en general y el delito de *hacking* en particular». *Revista Chilena de Derecho y Tecnología*, 3 (1): 11-78. DOI: 10.5354/0719-2584.2014.32220.

Muñoz, Fernando (2013). «Epistemología de la *techne*: A propósito del fraude informático». *Revista Chilena de Derecho y Tecnología*, 2 (2): 247-260. DOI: 10.5354/0719-2584.2013.30314.

Núñez, Raúl y Claudio Correa (2017). «La prueba ilícita en las diligencias limitativas de derechos fundamentales en el proceso penal chileno: Algunos problemas». *Ius et Praxis*, 23 (1): 195-246. DOI: 10.4067/S0718-00122017000100007.

Nogueira Alcalá, Humberto (2003). «El principio de reserva legal en la doctrina emanada del Tribunal Constitucional». *Ius et Praxis*, 9 (1): 541-544. DOI: 10.4067/S0718-00122003000100025.

—. (2005). «Aspectos de una teoría de los derechos fundamentales: La delimitación, regulación, garantías y limitaciones de los derechos fundamentales». *Ius et Praxis*, 11(2):15-64. DOI: 10.4067/S0718-00122005000200002.

Oxman, Nicolás (2013). «Estafas informáticas a través de internet: Acerca de la imputación penal del "phishing" y el "pharming"». *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, 41: 211-262. DOI: 10.4067/S0718-68512013000200007.

Pérez de Acha, Gisela (2016). *Hacking team: Malware para la vigilancia en América Latina*. Santiago: Derechos Digitales. Disponible en https://bit.ly/340jIAw.

Zapata, Patricio (2000). *La jurisprudencia del Tribunal Constitucional*. Santiago: Corporación Tiempo.

Zapata, María (2009). *La prueba ilícita*. Santiago: LexisNexis.

Sobre los autores

Valeria Ortega Romo es abogada. Licenciada en Ciencias Jurídicas y Sociales por la Universidad de Chile y diplomada en Regulación y Derecho Público por la misma institución. Su correo electrónico es val.ortega.r@gmail.com. http://orcid.org/0000-0001-9893-7974.

Pablo Viollier Bonvin es abogado. Licenciado en Ciencias Jurídicas y Sociales por la Universidad de Chile y diplomado en Ciberseguridad por la misma institución. Docente de la Facultad de Derecho de la Universidad Diego Portales, Chile. Su correo electrónico es pablo@derechosdigitales.org. http://orcid.org/0000-0003-2024-1453.

REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

La *Revista de Chilena de Derecho y Tecnología* es una publicación académica semestral del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, que tiene por objeto difundir en la comunidad jurídica los elementos necesarios para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en la ciencia jurídica.

EDITOR GENERAL

Daniel Álvarez Valenzuela
(dalvarez@derecho.uchile.cl)

SITIO WEB

rchdt.uchile.cl

CORREO ELECTRÓNICO

rchdt@derecho.uchile.cl

La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipográfica
(www.tipografica.cl).