Pre-INFORME

Aspectos técnicos y jurídicos del acceso a comunicaciones electrónicas en el marco de la persecución criminal y de medidas ejecutadas al amparo de la Ley Nº 19.974

Este Informe ha sido solicitado por la Defensoría Penal Pública a los profesionales que trabajan y colaboran con la organización no gubernamental Derechos Digitales, en su condición de especialistas en tecnología y la afectación de los derechos humanos por ella, en atención al interés público comprometido en el presente caso, y es firmado por la abogada doña María Paz Canales, Directora Ejecutiva de la organización, y por el Ingeniero Civil en Informática don Franco Castro, colaborador del área técnica de la organización. El pre-informe ha sido elaborado con la participación del equipo técnico de la organización integrado por don Israel Leiva y don Ignacio Espinosa, y por el Director de Investigación y Políticas Públicas de la organización, don J. Carlos Lara.

I. Sección Técnica

1. Acceso a las comunicaciones electrónicas a través de aplicaciones de mensajería Whatsapp y Telegram

1.1. Cómo funciona el cifrado de WhatsApp y Telegram

- **WhatsApp**

Desde el mes de abril del año 2016[1], WhatsApp utiliza una forma de cifrado de comunicaciones mediante la cual los únicos habilitados para acceder al contenido de las comunicaciones, incluyendo textos, videos, imágenes, archivos adjuntos y mensajes de voz, son las personas que participan de la conversación. Este tipo de cifrado, llamado cifrado de punto a punto[2], protege la información durante todo el viaje que hace el mensaje desde el dispositivo de origen hasta el dispositivo de destino, impidiendo que cualquier agente externo, incluyendo proveedores de internet o la misma compañía que provee WhatsApp, pueda acceder a él mientras el mensaje está en transito. Lo anterior es válido tanto para conversaciones individuales como grupales de la plataforma, y no puede ser deshabilitado en las configuraciones ni por el usuario ni por la empresa. Hasta la fecha no se conoce alguna falla pública en el protocolo que permita intervenir y acceder a los mensajes que se transmiten utilizando este cifrado.

[1] Ver https://blog.whatsapp.com/10000618/end-to-end-encryption
[2] Ver https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf
[2] Ver https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf

- **Telegram**

Telegram posee dos tipos de conversaciones que pueden estar protegidas por distintos tipos de cifrado: "Cloud Chats" y "Secret Chats"[3]. Los primeros son la configuración por defecto del sistema y protege el mensaje mientras está en tránsito desde el dispositivo de origen hacia los servidores de Telegram, y desde los servidores de Telegram hacia el dispositivo de destino, permitiendo a la compañía almacenar una copia no cifrada del mensaje para futuros usos, pero evitando al mismo tiempo que un tercero, como un proveedor de servicios de Internet, pueda acceder a la información en transito. Los mensajes enviados bajo la modalidad "Secret Chats" deben habilitarse manualmente como tales en la configuración del cliente y permiten enviar mensajes utilizando un cifrado punto a punto[4], protegiendo el contenido de estos de la observación que pudiese realizar un agente externo a la conversación, tales como un proveedor de servicios de Internet o la misma compañía Telegram. Esta modalidad de cifrado punto a punto sólo es posible para la comunicación entre dos individuos y no en conversaciones grupales.

1.2. ¿Es posible el acceso al contenido de las comunicaciones de Whatsapp y Telegram por el proveedor de tales aplicaciones?

En el caso de WhatsApp, no es posible para la compañía acceder al contenido de los mensajes enviados usando el cifrado de punto a punto mencionado en los párrafos anteriores. La única información que posee la compañía son los datos de la comunicación o meta-data, esto es, las cuentas (información de usuario y número telefónico) de origen y destino de los mensajes y las fechas en que estos fueron enviados. Por otro lado, es posible habilitar el respaldo de mensajes en el servicio en línea Google Drive, donde se guarda una copia de mensajes y archivos multimedia sin cifrar. Si esta opción se habilita, los datos de historial de chat son (en teoría) accesibles para la empresa Google, y sólo pueden ser recuperados si se tiene acceso a un smartphone con el mismo número de teléfono y cuenta de correo asociada.

En el caso de Telegram es posible para la compañia acceder al contenido de las comuncaciones si estas fueron realizadas bajo la modalidad "Cloud Chats", ya que estas no brindan protección de privacidad del contenido cuando se trata de la infraestructura y servidores de Telegram. En el caso de la modalidad "Secret Chats", no es posible acceder al contenido de las comunicaciones por parte de la compañia, la que sólo tendría acceso a los datos de la comunicación o meta-data de las mismas, vale decir: cuentas de origen y destino de los mensajes (información de usuario y número telefónico) y las fechas en que se efectuaron los envíos.

1.3. ¿Es posible el acceso al contenido de las comunicaciones de Whatsapp y Telegram por la compañía que presta servicios de acceso a internet?

Los proveedores de Internet no tienen la capacidad técnica de acceder al contenido de las comunicaciones mientras esta esté en transito entre los clientes de mensajería y los servidores

[3] Ver https://telegram.org/faq#secret-chats
[4] Ver https://core.telegram.org/api/end-to-end

de las compañias que brindan el servicio. Los cifrados que utilizan tanto Whatsapp como Telegram protegen el contenido de los mensajes en casos de intervención de las comunicaciones que atraviesan la infraestructura de los proveedores de servicio de internet, haciendo imposible que estos puedan entregar dicha información basándose sólo en el "monitoreo" de cuentas asociadas a personas específicas, como si ocurre con el servicio de telefonía.

2. Acceso a las comunicaciones electrónicas a través de uso de software espía (spyware)

2.1. Descripción de software espía que puede ser instalado en dispositivos para el acceso remoto a comunicaciones electrónicas

Un software espía (llamado spyware o malware) es un programa informático desarrollado con el propósito de tener acceso remoto a los datos y funcionamiento de un *smartphone*, sin que el dueño o dueña del dispositivo brinde su autorización, ni se percate de su presencia. Un software espía actúa de manera oculta y se encarga de recolectar información del dispositivo en el que está instalado, obteniendo información relativa a contactos del teléfono, chats de aplicaciones, imágenes, videos, etc. Generalmente, un software espía puede recolectar el historial de chat de aplicaciones populares como WhatsApp o Telegram. Además, un software espía se configura de manera tal que la información recolectada es enviada a un tercero a través de internet de manera periódica, como por ejemplo una vez al día. En algunos casos, si el *smartphone* se encuentra conectado a internet es posible acceder "en tiempo real" al dispositivo para extraer datos o vigilar las acciones de quien lo utiliza.

2.2. Formas en las cuales puede infectarse un dispositivo para el acceso remoto a comunicaciones electrónicas

La instalación de un software espía está fuera del alcance de las compañías de telefonía, proveedores de servicios o las empresas que manufacturan los dispositivos, como Google o Sony. Dicho esto, existen varias maneras de lograr la instalación:

- Si se tiene acceso físico al *smartphone*, se puede descargar el software espía desde algún sitio de internet o copiar desde un computador e instalar.

- Si no se tiene acceso físico al *smartphone*, se debe "forzar" al dueño del dispositivo a instalar el software espía o intervenir la conexión a internet utilizada por el dispositivo. Para esto, se engaña a la víctima para que lo instale sin que se de cuenta. Esto incluye:

a) Enviar un mensaje de texto o correo falso que invite a hacer *click* en un enlace a una página. Al abrir el enlace el *smartphone* descarga e instala el software espía sin que la víctima se percate;

b) Enviar un documento adjunto en un correo invitando a la víctima a descargar y abrirlo. El software espía viene oculto dentro del documento, y al abrir este último se concreta la instalación sin que la víctima lo note; y,

c) Interceptar y manipular la conexión de internet para enviar información falsa, requiriendo que el *smartphone* instale alguna actualización de sistema o derechamente forzando la instalación del software espía, aprovechando algún error en el dispositivo que brinde acceso para ello.

En cualquier caso, estos métodos no son infalibles y dependen de las características de cada *smartphone* y su mantención.

3. Otras formas de acceso físico a las comunicaciones electrónicas

Para el caso de WhatsApp, la aplicación guarda un respaldo de mensajes en el *smartphone*, por lo tanto si se tiene acceso físico al dispositivo y este no tiene un patrón de acceso, o si el patrón de acceso es conocido, es posible acceder a los historiales de chat utilizando programas públicamente disponibles en internet, siempre y cuando el contenido del *smartphone* no esté cifrado. Cabe mencionar que WhatsApp está diseñado para evitar este tipo de situaciones, por lo que es necesario generar comportamientos inesperados en el teléfono para lograr acceder a la información usando este método. Otra alternativa es utilizar el teléfono para vincular una cuenta a través de WhatsApp web y obtener acceso a todos los chats en tiempo real.

Para el caso de Telegram, la aplicación no guarda respaldo de mensajes en el *smartphone*. Sin embargo, es posible utilizar el teléfono para vincular una cuenta a través de Telegram Web y acceder a todo el historial de chats.

4. Uso de cuentas de Facebook y entradas de Wikipedia como medio de verificación de identidad

4.1. Características técnicas de Facebook que permiten la creación de perfiles sin acreditación fehaciente de identidad

La creación de una cuenta nueva en la red social Facebook, implica ingresar sólo los siguientes datos personales:

- Primer Nombre,
- Primer Apellido,
- Dirección de correo electrónica o número de teléfono móvil, y
- Contraseña.

Una vez ingresados los datos, la plataforma envía un código de verificación al correo electrónico o número de teléfono para validar que la persona tiene acceso al medio de contacto ingresado. Una vez ingresado el código de verificación recibido, se crea y valida la cuenta pudieron acceder a la modificación de perfil y demás características del servicio.

En ningún momento se valida que los nombres correspondan realmente a la persona que dice ser titular de la cuenta. Tampoco existe un proceso de verificación entre los nombres y el medio de contacto ingresado. Esto permite que cualquier persona que tenga acceso a un correo electrónico o número de teléfono móvil que no esté previamente registrado en la plataforma, pueda generar una nueva cuenta en la red social haciéndose pasar por un tercero.

4.2. Características técnicas de Wikipedia que permiten ediciones transitorias y sin necesidad de verificación de identidad del editor o veracidad de la información

Wikipedia es una enciclopedia libre de Internet que funciona de manera colaborativa en base a aportes de voluntarios repartidos por todo el mundo. En vez de tener un grupo editorial duro que decide el contenido de las distintas entradas, la plataforma funciona en base a discusión y consenso de los voluntarios interesados en el contenido. Esta característica permite que eventualmente la información expuesta sea vandalizada, se ingrese contenido sin verificar o sea falsa, lo que en la mayoría de los casos es remediado por otros voluntarios con prontitud.

Las personas que aportan en la edición de contenido pueden crear cuentas de usuario en la plataforma que les identifiquen o hacer modificaciones directamente sin la necesidad de una cuenta, en cuyo caso se utiliza su dirección de Internet IP para identificar al autor de los cambios en el control de versiones de la plataforma. Esto facilita y promueve la participación de voluntarios eventuales, pero también permite que individuos puedan hacer modificaciones inescrupulosas con facilidad registrando únicamente la dirección IP, la que no siempre es útil para identificar inequívocamente al autor real de los cambios.

Por lo anterior, es posible afirmar que desde un punto de vista técnico, ni Facebook, ni Wikipedia son plataformas tecnológicas que permitan acreditar de manera certera la identidad de una persona, ni la veracidad de la información contenida en ellas.

II. Sección Jurídica

1. El contenido de las comunicaciones electrónicas se encuentra cubierto por el derecho a la inviolabilidad de las comunicaciones (art. 19 Nº5) y el respeto a la vida privada (art. 19 Nº4) de la Constitución Política de la República.

El art. 19 de la Constitución Política de la República, dispone que *"la Constitución asegura a todas las personas*: (...) Nº 5 *La inviolabilidad del hogar y de toda forma de comunicación privada. El hogar sólo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley"*.

Como ha sido expresado por el Tribunal Constitucional, la inviolabilidad de las comunicaciones resulta esencial en un régimen constitucional y democrático, por cuanto apunta a la protección del ejercicio de otras libertades públicas:

> "(...) Con esta expresión ("inviolabilidad") se apunta a proteger dos bienes jurídicos simultáneamente.
> Por una parte, el de la libertad de las comunicaciones. El solo hecho de que las personas sepan que lo que transmitan a otros será grabado, interceptado o registrado, genera una inhibición de comunicarse. No hay libertad allá "dónde no hay expectativa de cierta inmunidad frente a

> indagaciones ajenas. Protegiendo el secreto de las comunicaciones, se defiende la libertad para entablarlas" (Jiménez Campos, Javier; La garantía constitucional del secreto de las comunicaciones; en Revista Española de Derechos Constitucional, año 7, Nº 20, mayo-agosto, p. 51). Además, la comunicación debe circular libremente. De ahí que este derecho permita el desarrollo de varias libertades, como la de empresa, la ideológica y política, etc.
> Por la otra, se protege el secreto de las comunicaciones. Esto es, se precave que terceros a quienes no va dirigida la comunicación, accedan a ella. De ahí que la inviolabilidad es una presunción *iuris et de iure* de que lo que se transmite es parte de la privacidad de las personas, por lo que la revelación de ello, independientemente de su contenido, vulnera el derecho a la privacidad (Nogueira, H.; ob. cit., p. 540).
> Lo que la garantía protege es la comunicación, cualquiera sea su contenido y pertenezca o no éste al ámbito de la privacidad o intimidad. El secreto se predica respecto de la comunicación. Por lo mismo, abarca el mensaje y los datos de tráfico (ruta, hora, fecha, sujetos, etc.). Y es indiferente la titularidad pública o privada del canal que se utilice."[5]

Asimismo, dada la textura abierta escogida por el Constituyente para proteger "toda forma de comunicación privada", goza de la protección constitucional cualquier comunicación de dicha naturaleza independiente del medio por la cual ella circule, lo que debe entenderse abarca las comunicaciones electrónicas que circulan a través de internet. Así lo ha entendido el Tribunal Constitucional al señalar: *"Que la expresión que utiliza la Constitución es "comunicación privada". La expresión "comunicación" es genérica. Comprende todo proceso de transmisión de mensajes entre personas determinadas a través de cualquier medio técnico (Jiménez, J., ob. cit., p. 42). Por lo mismo, abarca incluso aquella que se hace con signos, en clave, con gráficos, cifras, de cualquier manera en dos o más personas se transmitan mensajes (Cea, José Luis; ob. cit., p. 217). (...)".*[6]

Del mismo modo, tampoco la disposición constitucional acota las formas de vulneración posible de las comunicaciones, por lo cual propio de la evolución tecnológica del mundo actual, cualquier medio técnico materialmente disponible para acceder a comunicaciones electrónicas de naturaleza privada entre las partes participantes en éstas debe ser considerada una infracción a dicha garantía fundamental, si no se encuentra amparada en una norma de autorización legal que cumpla con los exigentes requisitos establecidos en el art. 19 Nº 26 de la Constitución. En efecto, nuevamente el Tribunal Constitucional ilustra el punto al señalar:

> "(...) La Constitución utiliza tres expresiones. Con la primera ("interceptar") se garantiza que no se suspenda o impida que las comunicaciones emitidas por alguien lleguen a destino. Con la expresión "abrir" se protege a que los documentos o las comunicaciones privadas puedan ser abiertas por terceros. Finalmente, "registrar" es examinar minuciosamente la comunicación o los documentos para encontrar algo que pueda estar oculto. (...)
> En todo caso, estas tres formas de vulnerar la inviolabilidad deben ser entendidas en forma amplia, abarcando cualquier acción que implique acceder a comunicaciones privadas. Así como la Constitución no quiso acotar el tipo de comunicaciones que protegía, designándolas genéricamente como "toda forma de comunicación privada", para evitar la obsolescencia ante estos nuevos mecanismos, tampoco quiso explicitar estas fórmulas de vulneración. Por eso su enumeración abierta.

[5] Sentencia del Tribunal Constitucional, 11 de septiembre de 2012, Rol Nº 2153-11. Considerando Trigésimo primero. Énfasis agregado, en adelante todos los énfasis en citas han sido agregados a menos que se indique expresamente lo contrario.
[6] Sentencia del Tribunal Constitucional, 11 de septiembre de 2012, Rol Nº 2153-11. Considerando Trigésimo segundo.

> Consecuente con ello, la interceptación, la apertura o el registro se pueden hacer por cualquier medio tecnológico idóneo para el medio de comunicación empleado."[7]

De lo anterior es posible concluir, siguiendo al Tribunal Constitucional, que bajo nuestro ordenamiento jurídico gozan de la protección concedida en el art. 19 Nº5 de nuestra Constitución cualquier forma de comunicación privada por medios electrónicos, y por tanto ellas se encuentran amparadas en su inviolabilidad contra cualquier forma o medio tecnológico de quebrantamiento que se disponga, que no cumpla (o exceda) las hipótesis de excepción taxativamente contempladas a nivel legal que permiten restringir su ejercicio.

Por otra parte, el art. 19 de la Constitución Política de la República también consagra en su Nº 4: "El respeto y protección a la vida privada y a la honra de la persona y su familia".

Las comunicaciones electrónicas son el medio a través del cual en la actualidad se desenvuelven gran parte de las interacciones familiares y sociales de los sujetos, por lo cual constituyen un vehículo primordial de ejercicio del derecho a la vida privada.

La doctrina nacional ha recogido distintas definiciones del concepto de privacidad. El profesor Corral la define como *"la posición de una persona o entidad colectiva personal en virtud de la cual se encuentra libre de intromisiones o difusiones cognoscitivas de hechos que pertenecen a su interioridad corporal y psicológica o a las relaciones que ella mantiene o ha mantenido con otros, por parte de agentes externos que, sobre la base de una valoración media razonable, son ajenos al contenido y finalidad de dicha interioridad o relaciones"*[8]. Por otro lado, el profesor Cifuentes define el derecho a la intimidad como *"el derecho personalísimo que permite sustraer a la persona de la publicidad o de otras turbaciones a la vida privada, el cual está limitado por las necesidades sociales y los intereses públicos, y para finalizar cualquier atentado contra la honra o la intimidad, dado ese carácter nuclear o íntimo, inseparable del yo o la personalidad, tiene una connotación constitucional grave y profunda, casi siempre irreversible y difícilmente reparable".*[9]

La jurisprudencia, por su lado, ha señalado que "el derecho a la intimidad es una emanación de la dignidad natural, intrínseca de todo ser humano"[10]. En el mismo sentido se ha pronunciado el Tribunal Constitucional al señalar que "*el respeto y protección de la dignidad y de los derechos a la privacidad de la vida y de las comunicaciones, son base esencial del desarrollo libre de la personalidad de cada sujeto, así como de su manifestación en la comunidad a través de los grupos intermedios autónomos con que se estructura la sociedad*"[11].

El acceso no (suficientemente) autorizado a las comunicaciones electrónicas constituye no sólo una infracción a la garantía de inviolabilidad de las comunicaciones, como ya se ha visto, sino que también de la protección de la vida privada de los titulares de tales comunicaciones, en cuanto ellas son un vehículo para desenvolver sus relaciones sociales, en el marco de relaciones que no están destinadas desde su origen por el sujeto emisor a ser conocidas más que por aquellos interlocutores a los cuáles el emisor a decidido otorgar acceso a su espacio de intimidad.

---

[7] Sentencia del Tribunal Constitucional, 11 de septiembre de 2012, Rol Nº 2153-11. Considerando Trigésimo sexto.
[8] CORRAL TALCIANI, H., La vida privada y la propia imagen como objeto de disposición negocial. Revista de Derecho, Univ. Católica del Norte, Nº8 (2001), p.161.
[9] CIFUENTES, S., El derecho a la vida privada. Tutela a la intimidad, La Ley, Buenos Aires, 2007, p. 19.
[10] Sentencia de la Iltma. Corte de Apelaciones de Concepción, 5 de agosto de 2013, Rol Nº 753-2013.
[11] Sentencia del Tribunal Constitucional, 28 de octubre de 2003, Rol Nº 389-2003.

La relevancia de la vulneración de las garantías constitucionales a la inviolabilidad de las comunicaciones y de respeto a la vida privada, es tanto inmediata, como mediata. Inmediata, como ya se ha visto por cuanto ambas han sido reconocidas por el Constituyente como pilar para asegurar la dignidad intrínseca de las personas a cuyo servicio debe encontrarse el Estado y sus agentes, pero también mediata, en cuanto ambas garantías resultan esenciales para que otros derechos fundamentales asociados al ejercicio de libertades públicas puedan ser garantizados en un Estado de Derecho y en una sociedad democrática.

La libertad de expresión, el derecho a reunión, e incluso la libertad de movimiento pueden llegar a depender en gran medida de la garantía de la inviolabilidad de las comunicaciones y de respeto a la vida privada, en tanto, el solo sometimiento de tales derechos a través de actos intrusivos ilegítimos restringe el comportamiento libre de los sujetos por la vía de la autocensura motivada por el legítimo temor de observación por parte de terceros o por represalias asociadas al contenido de tales comunicaciones. Si se quiere cautelar el ejercicio de derechos en un Estado de Derecho y sociedad democrática, resulta esencial someter a un escrutinio estricto las hipótesis de habilitación legal -y el ejercicio concreto de las mismas- que permiten condicionar el ejercicio, pero no hacer desaparecer la inviolabilidad de las comunicaciones y la privacidad.

2. Las medidas del art. 24 de la Ley Nº 19.974 requieren de especificidad conforme al art. 28, y no pueden usarse para fines que excedan los de inteligencia autorizados en el art. 23 de la misma ley.

En cuanto a las hipótesis de autorización para condicionar el ejercicio de la inviolabilidad de las comunicaciones, deben cumplirse los requisitos dispuestos por el art. 19 Nº 26 de la Constitución Política para la restricción de derechos fundamentales, esto es, debe satisfacer tres criterios: idoneidad, necesidad y proporcionalidad en sentido estricto[12]. El Tribunal Constitucional ha entendido este mandato en el sentido de asegurar a todas las personas que las limitaciones que se impongan no impliquen la completa erogación de los derechos fundamentales en cuestión, señalando a este respecto:

> "Que, en este sentido, es necesario reiterar el criterio que ha sostenido este tribunal en cuanto a que las disposiciones legales que regulen el ejercicio de estos derechos, deben reunir los requisitos de 'determinación' y 'especificidad'. El primero exige que los derechos que puedan ser afectados se señalen, en forma concreta, en la norma legal; y el segundo requiere que la misma indique, de manera precisa, las medidas especiales que se puedan adoptar con tal finalidad. Por último, los derechos no podrán ser afectados en su esencia, ni imponerles condiciones, tributos o requisitos que impidan su libre ejercicio"[13].

En concreto, el Tribunal Constitucional ha aceptado que la inviolabilidad de las comunicaciones puede romperse "en los casos y formas determinados por la ley". Pero bajo los siguientes presupuestos:

[12] ALEXY, R., "Teoría de los derechos fundamentales", Centro de estudios políticos y constitucionales, Madrid, 2002. p. 111-115.
[13] Sentencia del Tribunal Constitucional, Rol N°325. En el mismo sentido, roles N°s 78, 284, 370, 373, 379 y 388.

> "En primer lugar, tiene que haber una autorización legal. Esta norma es la única que permite la accesibilidad de las comunicaciones privadas. El propósito de esta exigencia es hacer previsible para los eventuales afectados una apertura de dichas comunicaciones.
> En segundo lugar, la ley debe definir "los casos" en que la autorización es posible. Eso implica que la ley debe establecer o listar situaciones y que la autoridad que dispone la autorización debe encuadrarse en estas causales. Por lo mismo, toda resolución que levante total o parcialmente la inviolabilidad, requiere ser motivada.
> Es decir, debe establecer las razones que llevan a hacerlo y cómo éstas se ajustan a dichas causales o situaciones.
> En tercer lugar, es necesario que la ley defina "las formas" en que la autorización se puede dar. Esta expresión apunta, de un lado, a que la ley debe señalar el procedimiento que debe seguirse; del otro, las formalidades que debe adoptar la autorización.
> Finalmente, los casos y las formas deben estar "determinados". Es decir, deben estar establecidos o fijados de modo preciso, no genéricamente. (...)"[14]

El título V de la Ley Nº 19.974 determina los procedimientos especiales de obtención de información por los organismos de inteligencia. A este respecto, el art. 23 es clarísimo en señalar que la información a recabar debe resultar "estrictamente indispensable para el cumplimiento de los objetivos del Sistema y no pueda ser obtenida de fuentes abiertas", imponiendo con ello un deber de calificación de más elevado estándar para la aplicación de tales procedimientos.

El principio de "utilización exclusiva de la información" fue reconocido consistentemente por el legislador desde el inicio de la tramitación del Proyecto de Ley que se convirtió en la Ley Nº 19.974. En efecto en el mensaje presidencial que le dio origen se consigna:

> "Finalmente, se establece que los estudios, antecedentes, informes, datos y documentos que obtengan, elaboren, recopilen o intercambien los órganos que forman el Sistema de Inteligencia del Estado y su personal, sólo puede ser usado para el cumplimiento de sus respectivos cometidos".[15]

La exigencia estricta del art. 23 se refuerza con lo dispuesto en el inciso segundo del art. 28 de la misma ley, al imponer como requisitos esenciales de la autorización judicial otorgada por un Ministro de Corte de Apelaciones competente, que dicha resolución debe incluir "especificación de los medios que se emplearán", además de la individualización de las personas a quienes se aplica la medida y las limitaciones temporales de su aplicación.

El Tribunal Constitucional en su sentencia Rol Nº 2153-11, luego de referirse a la facultad de recabar información para fines de inteligencia contemplada en la Ley N° 19.974, atiende a las limitaciones contempladas en ésta que condicionan el ejercicio de tales facultades como un elemento esencial para el adecuado balance con la protección de la garantía de inviolabilidad de las comunicaciones, concluyendo a este respecto que:

> "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

[14] Sentencia del Tribunal Constitucional, 11 de septiembre de 2012, Rol Nº 2153-11. Considerando Trigésimo octavo.
[15] Historia de la Ley Nº 19.974. Mensaje Presidencial, p.12.

> 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);

Que, de este modo, el acceso a comunicaciones privadas sólo puede permitirlo el legislador cuando sea indispensable para una finalidad de relevancia mayor; cuando no haya otra alternativa disponible; bajo premisas estrictas; con una mínima intervención y nunca de manera constante y continua, sino que de forma limitada en el tiempo y siempre de modo específico, señalándose situaciones, personas, hechos."[16]

Durante la tramitación legislativa de la Ley Nº 19.974, el Senador Larraín consignó para la historia de la ley las preocupaciones que ésta abría en materia de respeto a la privacidad y la inviolabilidad de la comunicaciones, expresando:

> "A este respecto, se está efectuando una solicitud de información sin que necesariamente haya delito y, por tanto, se está abriendo un espacio de acceso a la vida privada de las personas, a mi juicio, sin tener claridad en el ámbito en el cual éste puede ejercerse. De manera que no me parece suficiente que la competencia se entregue a un ministro de la Corte de Apelaciones respectiva, porque todavía eso es demasiado discrecional. Acá hay un tema en extremo delicado, precisamente porque los procedimientos que podrá ordenar, sin que haya un juicio de por medio o un delito que se esté investigando, serán simplemente por la decisión discrecional de un servicio de inteligencia. Creo que esta materia deberemos revisarla con mucho cuidado cuando analicemos el proyecto en particular". [17]

Las preocupaciones de eventuales excesos respecto del uso de las facultades concedidas en la ley en discusión también fueron manifestadas por el Senador Espina:

> "Entonces, es necesario tener cuidado con estas normas, que pueden ser extraordinariamente invasivas. Siempre hemos estado muy llanos a que se adopten todas las medidas del caso para prevenir la ocurrencia de delitos y sancionar a los responsables de un ilícito grave; pero debemos ser muy cautelosos y evitar que esas disposiciones terminen haciéndonos vivir en una especie de sociedad donde cualquier paso, movimiento o acción de una persona pueda ser objeto el día de mañana de graves invasiones o interferencias en su vida privada y en el legítimo derecho de tenerla y mantenerla en tal carácter.
> Desde ese punto de vista, pienso que estos preceptos deben ser objeto de acuciosa revisión antes de otorgar las facultades que se entregan, a fin de evitar que en el futuro, por haberlas concedido con demasiada facilidad, se puedan prestar a un mal uso e infligir grave daño a las labores de inteligencia que se requiera realizar."[18]

Las órdenes judiciales emitidas por el Ministro Sr. Aner Padilla en su calidad de Ministro designado según el artículo 25 de la Ley N° 19.974, según Acuerdo del Tribunal Pleno de la Corte de Apelaciones de Temuco N° 6-2017 de 3 de enero de 2017, con fecha 9 de agosto de 2017 y 7 de septiembre de 2017 (en adelante "las Órdenes"), autorizan respecto de las personas que en ellas se señalan a:

> "la intervención de cualesquiera otros sistemas tecnológicos destinados a la transmisión, almacenamiento o procesamiento de comunicaciones o información, para que el personal de la

[16] Sentencia del Tribunal Constitucional, 11 de septiembre de 2012, Rol Nº 2153-11. Considerando Cuadragésimo y cuadragésimo primero.
[17] Historia de la Ley Nº 19.974. Discusión en sala, p.241.
[18] Historia de la Ley Nº 19.974. Discusión en sala, p.245.

> Dirección Nacional de Inteligencia, Drogas e Investigación Criminal de Carabineros de Chile pueda realizar diligencias o acciones de Inteligencia con la finalidad de procesar sistemáticamente la recolección, evaluación y análisis de las comunicaciones e información relevante que se obtenga de aplicaciones telefónicas de WhatsApp, Telegram, Facebook y cuentas de correos electrónicos que se encuentren asociados a los números y respecto de las personas que se indican, incluso aquellas comunicaciones e informaciones relevantes a las que se tenga acceso o se puedan obtener, y que se hayan producido o generado con una antelación máxima de 30 días, contados desde esta fecha y hora.
> Se autoriza que estas diligencias o acciones de Inteligencia se inicien en la ciudad de Temuco, y dentro del territorio jurisdiccional de esa Ilustrísima Corte de Apelaciones, por el plazo de noventa días, desde esta fecha y hora".

Resulta muy dudoso que tal autorización satisfaga el requisito de "especificación de los medios que se emplearán" exigido por el art. 28 Ley N° 19.974, con la con la sola enunciación del tipo de comunicaciones que pueden ser accedidos en virtud de tal orden por los servicios de inteligencia, pero **sin especificar los medios por los cuales ello se hará**, los cuales como se aprecia del capítulo técnico del presente informe pueden ser de diversa índole técnica, con diversa forma de afectación de las garantías constitucionales de inviolabilidad de las comunicaciones y derecho a la vida privada de los sujetos afectadas por ellas. Además, vulnerando el plazo máximo considerado en la misma disposición se autoriza un **efecto retroactivo de la autorización**, que excede el marco legal que sólo contempla efecto hacia el futuro de las autorizaciones por un plazo máximo de 90 días.

Finalmente, y lo que resulta más relevante -como se verá en el apartado siguiente- es que la información obtenida de una acción de inteligencia como la autorizada por las Órdenes, carece totalmente de legalidad como prueba dentro de un proceso penal sin una autorización de parte del Juez de Garantía competente, y a la vez infringe y excede gravemente los principios plasmados en la Ley N° 19.974 y tenidos en cuenta por el legislador a la hora de aprobar las facultades excepcionales que en ella se contemplan que permiten la restricción, más no la conculcación de las garantías fundamentales de inviolabilidad de las comunicaciones y respeto a la vida privada.

3. Una orden de interceptación de comunicaciones al amparo del art. 222 del Código Procesal Penal, aplicada a comunicaciones electrónicas, no cubre el registro del contenido de la comunicación interceptada, sino tan solo los datos comunicacionales de la misma.

Existen al menos dos hipótesis de acceso remoto (esto es, sin a las comunicaciones mediante mensajes enviados a través de servicios de mensajería instantánea. Una es la interceptación de dichos mensajes en los términos antes descritos de forma sincrónica o simultánea a su desarrollo. La segunda es el acceso a los registros (*logs*) de esas comunicaciones, que pudieren estar (en caso de existir) en poder de los proveedores de tales servicios de mensajería.

Los artículos 222 y siguientes del Código Procesal Penal disponen las reglas bajo las cuales las comunicaciones telefónicas y de otro tipo pueden ser interceptadas, esto es, capturadas en tránsito para conocer su contenido. Conforme al art. 222, "Cuando existieren fundadas sospechas, basadas en hechos determinados, de que una persona hubiere cometido o participado en la preparación o comisión, o que ella preparare actualmente la comisión o participación en un hecho punible que mereciere pena de crimen, y la investigación lo hiciere

imprescindible, el juez de garantía, a petición del ministerio público, podrá ordenar la interceptación y grabación de sus comunicaciones telefónicas o de otras formas de telecomunicación". Reza el segundo inciso que "La orden a que se refiere el inciso precedente sólo podrá afectar al imputado o a personas respecto de las cuales existieren sospechas fundadas, basadas en hechos determinados, de que ellas sirven de intermediarias de dichas comunicaciones y, asimismo, de aquellas que facilitaren sus medios de comunicación al imputado o sus intermediarios". De lo anterior se coligen requisitos para la procedencia de tal interceptación,

El inciso quinto del artículo 222 del Código Procesal Penal establece las condiciones bajo las cuales un proveedor de servicios de internet o empresa de comunicaciones debe retener ciertos datos sobre comunicaciones (conocidos también como "metadatos"), para eventualmente entregarlos en el contexto de una investigación penal. Esa obligación no alcanza a regular los registros del contenido de las comunicaciones.

El art. 222 del Código Procesal Penal no autoriza, ni establece requerimientos específicos, para el acceso a los registros de los contenidos de comunicaciones privadas que pudieren estar almacenados en ordenadores (servidores) de los proveedores del servicio de comunicaciones. Por estar limitada la regulación a la interceptación y la grabación de comunicaciones de forma sincrónica, las comunicaciones asíncronas están patentemente fuera de la regulación. De ello no se deduce que no puedan adoptarse medidas para el acceso a esos registros (por ejemplo, de forma análoga a la incautación de correo regulada en el artículo 218). No obstante, en atención a las reglas generales sobre tutela de garantías, como también la amplia regulación sobre las demás formas de interceptación de las comunicaciones, cualquier autorización relativa a los registros de comunicaciones privadas debe cumplir, a lo menos, con los requisitos sobre sospechas fundadas, basadas en hechos determinados, relativas a la comisión o preparación de un hecho punible con pena de crimen, y con expresas limitaciones temporales y de contenidos, bajo solicitud del Ministerio Público y autorización expresa del juez de garantía, en orden dirigida a quienes cuenten con tal registro. No consta que tal autorización hoy exista en el caso de autos.

De acuerdo con el art. 224, la interceptación debe ser notificada a los afectados con posterioridad a su realización. No existen antecedentes claros de la práctica de la notificación a la red de personas cuyas comunicaciones aparecen como intervenidas por parte de Carabineros, con lo que la medida incumple los requisitos legales para su procedencia y mantiene su carácter de irregular.

Como consecuencia de lo anterior, una orden de interceptación de comunicaciones al amparo del art. 222 del Código Procesal Penal, no puede ser aplicada a la interceptación directa de las comunicaciones electrónicas cifradas, incluidos los servicios de mensajería como WhatsApp, Telegram y otros.

4. El uso de software espía (spyware) constituiría una infracción a la Ley Nº 19.223 Que tipifica figuras penales relativas a la informática.

De conformidad con el art. 2° de la Ley Nº 19.223, "El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma,

lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio". Conforme a la disposición citada, acceder, interceptar o interferir con un sistema de comunicación, tal como lo es un servicio de mensajería, constituirá delito. Esta hipótesis delictual es conocida como acceso no autorizado, intromisión informática o espionaje informático.

La disposición en comento contempla como elemento normativo del tipo "usar... **indebidamente**" la información. De lo anterior se deduce que el tipo se cumple al no existir autorización para el ingreso. Dicha autorización puede tomar la forma de facultad legal para la interceptación, interferencia o acceso, como lo sería la presencia de una autorización legal expresa, como la contemplada en los artículos 222 y ss. del Código Procesal Penal, o las hipótesis de intervención de la Ley Nº 19.974 antes citada. Puesto que dicha autorización no consta de los antecedentes puestos a disposición de la defensa en este caso, la intervención a partir de la cual se ofrecen antecedentes a modo de prueba constituye una hipótesis de espionaje informático.

La expresión "indebidamente" ha sido interpretada por parte de la doctrina como asociada a la superación de una barrera técnica[19]. En atención al carácter cifrado de las comunicaciones ya referidas, no existe constancia de que se haya producido una forma de intervención permitida voluntariamente por los participantes en la comunicación, con lo que la superación de barreras técnicas (*hacking*) para el acceso aparece como necesaria. Aun prescindiendo del punto anterior, se trata de la realización del tipo penal ya referido, con lo que la intervención de las comunicaciones sería constitutiva de delito.

En virtud de las reglas constitucionales fijadas en el Artículo 19 Nº 7 de la Constitución Política de la República, y de los artículos 5º y 9º del Código Procesal Penal, es perentorio que la condena, así como también la adopción de medidas cautelares restrictivas de derechos fundamentales, se funde en pruebas lícitamente obtenidas y practicadas con las debidas garantías procesales. La ausencia de cumplimiento de tales garantías significa no solamente la inviabilidad del uso a modo de prueba o de antecedente para la adopción de las medidas cautelares, sino también la comisión de un delito. Un procedimiento lícitamente tramitado no puede fundarse en medidas que a su vez constituyen delito.

III. Conclusiones

De la información disponible, no es posible sostener que se hayan cumplido en el acceso las comunicaciones electrónicas de los imputados los requisitos legales para que la recolección de antecedentes sirvan para determinar la participación de los imputados en la comisión o preparación de delitos. Si tanto la investigación que recae sobre ellos como la adopción de medidas cautelares restrictivas de libertad se basan en tales antecedentes, tales actuaciones se encuentran viciadas. El desconocimiento de la totalidad y el detalle de las interceptaciones que dan pie a la restricción de libertad en este caso, configuran una hipótesis de indefensión contraria a los derechos consagrados en la Constitución y en los tratados internacionales sobre derechos humanos.

[19] Medina, G., "Estructura típica del delito de intromisión informática", *Revista Chilena de Derecho y Tecnología* vol. 3 Nº 1, 2013, pp.79-99.

Las Ordenes de autorización para la intervención de comunicaciones bajo la Ley Nº 19.974 no cumplen con el requisito de "especificación de los medios que se emplearán" exigido por el art. 28 de la misma ley, además de vulnerar el plazo máximo que sólo contempla efecto hacia el futuro, por hasta noventa días.

La autorización para la interceptación de comunicaciones bajo la Ley Nº 19.974 es además en cualquier caso insuficiente para generar antecedentes que permitan llevar adelante una persecución penal bajo el Código Procesal Penal, pues la información obtenida de una acción de inteligencia como la autorizada carece totalmente de legalidad como prueba dentro de un proceso penal sin la autorización expresa de parte del Juez de Garantía competente.

La interceptación de comunicaciones y la mantención de registros de las mismas no solamente es irregular desde el punto de vista procesal, sino que además constituye delito un informático, que no puede constituir la base de una persecución penal, y que por sí solo representa una vulneración sustantiva de los derechos fundamentales de los afectados.

Es lo que podemos informar. Quedamos a vuestra disposición para aclarar y ampliar cualquier aspecto relacionado con el presente pre-informe.

Saludan atentamente a Ud.,

MARÍA PAZ CANALES
Abogada, Universidad de Chile
Magíster en Derecho y Tecnología,
Universidad de California, Berkeley

FRANCO CASTRO
Ingeniero Civil Informático
Universidad Técnica Federico Santa María

Santiago, 3 de octubre de 2017