Revista Judicial, Poder Judicial de Costa Rica, Nº 129, págs 167 - 178 ISSN 2215-2377 / Diciembre 2020

VIGILANCIA ELECTRÓNICA DE LAS COMUNICACIONES A LA LUZ DE NUESTRA NORMATIVA: REALIDADES Y DESAFÍOS

M.Sc. Mario de Jesús Jiménez Aguilar *

RESUMEN

El presente artículo pretende ofrecer algunas ideas elementales sobre los nuevos desafíos normativos y prácticos a los que se enfrentará Costa Rica de cara a la implementación de la vigilancia electrónica en la investigación del crimen organizado, considerando los aportes del Convenio de Budapest sobre Ciberdelincuencia de 2001 y las experiencias de países como Estados Unidos, Brasil, Francia o Australia, de tal suerte que las reformas legislativas que se planteen encuentren un justo balance entre dotar a las autoridades policiales de herramientas ágiles y eficaces a la altura de la era digital en el combate al crimen organizado y la necesaria tutela de los derechos fundamentales.

Palabras clave: *Interceptación de las comunicaciones, crimen organizado, redes sociales, vigilancia electrónica, derechos fundamentales.*

ABSTRACT

This article will offer readers elemental ideas about next challenges in law reforms would face Costa Rica with electronic surveillance on organized crime investigations, considering regulatory provisions of the Budapest Convenant of 2001 and experiences of countries as United States, Brazil, France or Australia, in such a way as new law reforms allow investigators prosecute organized crime with efficient technology tools but in a total respect of Constitutional rights involved.

Key Words: *Comunications tapping, organized crime groups, social media, electronic surveillance. constitutional rights.*

Recibido 7 julio 2020 *Aprobado 12 agosto 2020*

* *Máster en Administración de Justicia Penal, Universidad Nacional de Costa Rica; licenciado en Derecho por la Universidad de Costa Rica; juez contralor propietario, Centro Judicial de Interceptación de las Comunicaciones CJIC. mjimenezag@poder-judicial.go.cr.*

Volver al índice

I. Introducción

El auge cada vez más creciente en la intercomunicación global impact**ó** positivamente en la vida de las personas usuarias de las distintas tecnologías de la información al permitirles, desde cualquier latitud, la adquisición de bienes y servicios con solo un *clic*: basta contar con un *smartphone*, *tablet* o cualquier otro "dispositivo inteligente" y acceso a Internet para descubrir un mundo cibernético abrumado de ofertas atractivas para las personas navegadoras.

El mundo de los negocios -y aun el de las relaciones interpersonales- dieron un giro significativo desde la génesis de las redes sociales (RRSS) y las aplicaciones (*Apps)*, acuñándolas como los medios de comunicación predilectos por la gran mayoría de personas usuarias.

Es cada vez más frecuente la reserva de boletos de avión u hoteles de descanso desde páginas de Internet oficiales o a través de *buscadores* que empleando los añejos métodos como la llamada telefónica, habida cuenta de que es mucho más económica e informadora que aquella.

Pese ello, también es un hecho que dichas herramientas son cada vez más empleadas por los y las ciberdelincuentes para la comisión de hechos ilícitos, aprovechando las facilidades del anonimato y el contexto de acción criminal *(ciberespacio)* que les proporcionan estas tecnologías.

Delitos graves como la pornografía infantil y la corrupción de menores, estafas mayores, tráfico de personas, tráfico de estupefacientes o legitimación de activos son algunas de las conductas delictivas, cuyos autores, autoras y partícipes encuentran en las *RRSS* y *Apps* un vehículo gratuito, ágil y anónimo para la transmisión de datos y de alcance global para consumar sus fines, dificultando, en muchos casos, la oportuna acción policial y, con ello, propiciar terreno fértil para la impunidad.

La imposibilidad de interceptar en tiempo real el contenido de las comunicaciones que se materializan vía Internet o correos electrónicos ofrece al crimen organizado ventajas de gran envergadura que deben llamar profundamente la atención sobre la existencia de leyes obsoletas o adecuadas para la nueva era de la información; pero sin mayor aplicación práctica, anteponiendo claro está, los derechos fundamentales de la ciudadanía como límite al poder público.

En este artículo, se expondrán brevemente las experiencias legislativas de países "pioneros" en este tema, así como los alcances de la normativa imperante en Costa Rica y sus desafíos en punto a la cada vez más necesaria interceptación en tiempo real, los datos contenidos en redes sociales, aplicaciones, correos electrónicos de los autores, las autoras o partícipes de delitos graves.

II. La interceptación de las comunicaciones telefónicas: el método clásico

La Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones, N. º7425 del 9 de agosto de 1994 y sus reformas, así como Ley contra la Delincuencia Organizada y sus enmiendas, N.° 8754 del 24 de julio de 2009, constituyen el texto legal base que faculta a las autoridades jurisdiccionales a ordenar y ejecutar la interceptación de las comunicaciones privadas en tiempo real a cargo de la persona juzgadora territorial o, cuando así lo disponga, por delegación al Centro Judicial de Intervención de las Comunicaciones (CJIC).

Volver al índice

Como derivado de los límites que impone el canon 24 Constitucional[1], estas potestades intrusivas del poder público solo resultan procedentes en la investigación criminal de delitos graves y con absoluta supervisión jurisdiccional. La experiencia forense actual señala que dicho centro, cuya naturaleza es eminentemente jurisdiccional, ubica su actividad en la escucha y discriminación de comunicaciones telefónicas que se materializan a través del desvío de líneas convencionales que las operadoras telefónicas ejecutan por mandato.

Empero, esa misma experiencia apunta a una utilización cada vez más acentuada de herramientas electrónicas a cargo de personas autoras y partícipes de delitos graves, como instrumentos de fácil acceso y dotados de total confidencialidad que terminan obstaculizando la acción policial oportuna.

En ese sentido, conviene examinar si Costa Rica cuenta con una legislación y recursos prácticos para lograr una adecuada vigilancia sobre la actividad criminal más allá de aquella que se verifica actualmente mediante la interceptación de comunicaciones telefónicas.

No está de más recordar, que ambos textos legales (Leyes 7425 y 8754) autorizan la interceptación de medios *digitales* y *electrónicos*[2], dentro de los límites establecidos por la misma normativa, pero se carece de una descripción sobre qué mecanismos de ejecución práctica sustentarán estas labores de vigilancia, lo que parece que deja vacío de contenido a dicho articulado. No es extraño escuchar que el crimen organizado "va un paso adelante" de la acción policial en sentido tecnológico. Esta afirmación bien podría ser cierta en la medida en que se sigan empleando los mismos mecanismos de comprobación delictiva que, aunque legítimos, parecen seguir siendo insuficientes.

III. La vigilancia electrónica según el Convenio de Budapest sobre Ciberdelincuencia de 2001

Mediante Ley de la República N.º 9452 del 26 de mayo de 2017, vigente a partir del 1 de enero de 2018, Costa Rica se adhiere al **Convenio de Europa sobre Ciberdelincuencia o Convenio de Budapest de 2001,** en el cual los Estados suscribientes se comprometen a establecer en sus ordenamientos internos las herramientas jurídicas necesarias para combatir los delitos informáticos *per se* o cuando constituyan el medio para cometer otros ilícitos graves. En términos generales, el Convenio hace un balance entre la necesidad de tipificar conductas criminosas cometidas en el *ciberespacio* y la urgida protección de los datos contenidos en los "sistemas informáticos", incluso con sanciones también punitivas para quienes vulneren ilegítimamente la privacidad de su contenido.

Cabe destacar, que con arreglo al artículo 1[3], existen cuatro definiciones básicas que informan

1 *El numeral 24 Constitucional en lo que interesa:"garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones […] Igualmente la Ley determinará en cuáles casos podrán los Tribunales de Justicia ordenar que se intervenga cualquier tipo de comunicación e indicará los delitos en cuya investigación podrá autorizarse el uso de esta potestad excepcional y durante cuánto tiempo […] Las resoluciones judiciales amparadas a esta norma deberán ser razonadas y podrán ejecutarse de inmediato. Su aplicación y control serán responsabilidad indelegable de la autoridad judicial […]". Constitución Política de la República de Costa Rica, en http://www.pgrweb.go.cr/, consultada el 2/13/19.*

2 *Los artículos 9 de la Ley 7425 y 15 de la Ley 8754 de Costa Rica catalogan como documentos privados los contenidos digitales y electrónicos del ciberespacio. Consultados en* http://www.pgrweb.go.cr/, el 2/13/19.

3 *Convenio de Budapest sobre Ciberdelincuencia de 2001, consultado en* http://pgrweb.go.cr/ *el 2/13/19.*

Volver al índice

dicho instrumento y que pueden resumirse de la siguiente forma: a) "sistema informático" entendido como todo dispositivo aislado o intercomunicado que permite la ejecución de un programa; b) "datos informáticos" que consisten en todo contenido representativo de hechos que hace posible la comunicación; c) el "proveedor de servicios" que alude a cualquier entidad pública o privada que ofrezca a las personas usuarias posibilidades de comunicación o que procese o almacene datos informáticos y los "datos de tráfico" que son todos aquellos que sin revelar el contenido de la información, sí detallan aspectos referenciales tales como: origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación.

Para una mejor comprensión, dentro de "sistema informático", se incluirán la Internet, redes sociales, aplicaciones y cualquier otro dispositivo informático afín de que permitan el almacenamiento y comunicación de datos; el "dato informático" como el contenido privado y más sensible en el fenómeno de trasmisión de datos electrónicos y los "datos de tráfico" como aquellos que sin ser estrictamente confidenciales ofrecen información sobre los movimientos comunicativos entre las personas usuarias, incluyendo su geolocalización.

En lo conducente a los proveedores del servicio, estos deberán incluir no solo las operadoras locales de servicios de Internet (en Costa Rica, Kolbi, Claro, Movistar), sino también las grandes compañías extranjeras administradoras de redes sociales y aplicaciones de alta demanda (*Facebook, Whastapp, Messenger*, entre otras).

Ahora bien, a efectos de dar cumplimiento a los objetivos de este artículo, nos limitaremos a examinar los alcances del Convenio sobre la obtención en *tiempo real* de los datos de tráfico y los datos informáticos. En lo concerniente a los ***datos de tráfico***, el artículo 20 del citado Convenio reseña en lo que interesa:

> *cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a: obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio y b. obligar a un proveedor de servicios, dentro de los límites de su capacidad técnica: i. obtener o grabar mediante la aplicación de medios tecnológicos existentes en su territorio o, ii. Prestar a las autoridades competentes su asistencia para obtener, grabar en tiempo real, los datos sobre el tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.*

Como se apuntó líneas atrás, estos datos no aluden al contenido privado de la información, aunque no por ello, quedan excluidos de la tutela del canon 24 Constitucional sobre el derecho fundamental al secreto y a la privacidad de los documentos y las comunicaciones privadas. Pese a su naturaleza estrictamente *referencial*, estos datos sí brindan información valiosa que permite a las autoridades policiales, al menos, conocer la hora y fecha exactas en que se ejecuta la transmisión de datos o aun la *geolocalización* de la persona usuaria, proporcionando algunos datos sobre su ubicación actual.

En lo atinente a la interceptación de *datos informáticos* o *"**datos de contenido"**,* el numeral 21 del mismo Convenio refiere en lo conducente que:

> *cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a las autoridades competentes, por lo que respecta a una serie de delitos graves que deberán definirse en su derecho interno: a) a obtener o grabar mediante la aplicación de medios técnicos*

Volver al índice

> *existentes en su territorio; y b)* ***obligar a un proveedor de servicio dentro de los límites de su capacidad técnica****: i. a obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio; ii. a prestar a las autoridades competentes su asistencia y su asistencia para grabar* ***en tiempo real, los datos sobre el contenido de determinadas comunicaciones en su territorio****, transmitidas por medio de un sistema informático […] (énfasis es propio).*

Sobre el particular, creemos importante anotar las siguientes limitaciones de orden jurídico y pragmático:

1) **La obligatoriedad al proveedor de los servicios de Internet se condiciona según su capacidad técnica.** Hoy día, los instrumentos de tecnología de la información que gozan de mayores ventajas a sus usuarios y usuarias por la versatilidad de sus funciones en la transmisión de datos informáticos y por su encriptación de extremo a extremo (*Facebook, Messenger y Whatsapp*) no son propiedad de las personas proveedores de los servicios en cada país, sino de una empresa multinacional domiciliada en los Estados Unidos de Norteamérica y liderada por Mark Zuckerberg, fundador de *Facebook*. Esta compañía ha hecho patente su política de no facilitar información privada como parte de su estrategia comercial para atraer y conservar a sus cientos de millones de usuarios y usuarias diarios.

Recientemente, la compañía adquirió la red social *Whatsapp* por un total de 17 000 millones de euros[4], lo que confirma el monopolio casi total que ejerce esa empresa transfronteriza de tráfico de datos. En este panorama, parece que los "proveedores de servicio local" poco o nada podrían hacer para lograr la recopilación de datos informáticos emanados de las redes sociales o aplicaciones que facilitan a sus usuarios y usuarias y, con ello, podrían invocar "la incapacidad técnica" que sugiere el mismo Convenio.

En el 2016, la comunidad internacional conoció que personas juzgadoras brasileñas ordenaron el bloqueo de la red de mensajería instantánea *Whatsapp* por un plazo de 72 horas ante la negativa de Diego Dzodan, ejecutivo de *Facebook* para Latinoamérica, de entregar comunicaciones privadas de personas sospechosas integrantes de una organización criminal en el marco de una investigación por tráfico de drogas.

Según se informó, los sujetos empleaban el *Whatsapp* para fraguar por este medio y no por líneas telefónicas convencionales, los distintos aspectos de logística, coordinación y ejecución de las actividades ilícitas[5]. Al final, el tribunal *ad quem* anuló lo resuelto en primera instancia entre otras razones válidas, por ser una medida desproporcionada.

2) **El problema de la eficacia pragmática del Convenio.** Si la tendencia actual de los directivos de estas grandes empresas multinacionales es negar la entrega de información privada, ¿existen los remedios legales en el plano internacional para compelerlas? El Convenio está informado a lo largo de su contenido, del llamado a los Estados parte para incluir legislación que permita constreñir "a los proveedores de

4 *Suárez Eduardo. "Facebook compra WhatsApp por 19.000 millones de dólares". Diario El Mundo (Nueva York, 02/20/2014), página web* https://www.elmundo.es/, *accedido el 7/20/19*

5 *"¿Por qué Brasil se quedó sin WhatsApp por orden judicial?". Diario BBC Mundo (Nueva York, 02/05/2016), página web* www.bbc.com/, *accedido el 7/19/19*

Volver al índice

los servicios" tanto para la entrega de datos por ellos almacenados –sean de tráfico o informáticos- como los que se verifiquen *en tiempo real,* mas no se incorpora una eventual solución al problema subyacente.

3) **Los problemas de inversión en infraestructura y personal humano.** Los datos informáticos que deben evaluarse se contarán por miles o decenas de miles diariamente, dada la naturaleza de *mensajería rápida* que revisten aplicaciones como *Whatsapp*. Esto obligará a replantearse el tema sobre la necesaria inversión en infraestructura y personal jurisdiccional (al menos para el caso de Costa Rica) que permita dar abasto con toda la información que es recibida.

Debe recordarse que el CJIC, como órgano contralor de legalidad, debe encargarse además de la comunicación oportuna a los oficiales encargados sobre los movimientos delictivos que realicen los intervenidos, a fin de que las autoridades policiales puedan no solo incorporar válidamente prueba al proceso (*v. gr.* a través del decomiso de evidencia), sino también la evitación de la comisión de otros hechos delictivos, por lo que la capacidad de respuesta del CJIC debe ser siempre oportuna.

IV. Los casos de EEUU y Francia: ¿el fin justifica los medios o vulneración flagrante a derechos fundamentales?

A menos de dos meses de sucedidos los atentados terroristas del 11 de septiembre de 2001, el Senado de los Estados Unidos de Norteamérica aprobó casi por unanimidad la llamada Ley *Patriot Act* que alude al acrónimo *Providing Appropiate Tools Required to Intercept and Obstruct Terrorism (PATRIOT*), la cual vendría a otorgarles poderes casi absolutos al director del FBI y a sus oficiales para ejercer mayores controles sobre la vigilancia electrónica *(electronic surveillance)* de terroristas y no terroristas[6]. Gracias a su aprobación, se podría ahora activar estas nuevas herramientas a delitos informáticos *(mail fraud; passport fraud)*, tráfico de drogas o el *blanqueo* de activos, lo que supuso que el FBI podía contar con instrumentos informáticos que permitieran el "espionaje masivo" a la ciudadanía sin control jurisdiccional.

Esta hipótesis se confirmó en el 2013, cuando Edward Snowden reveló una enorme red de espionaje de los Estados Unidos tanto a la ciudadanía como a otras naciones a cargo de la Agencia de Seguridad Nacional *(NSA,* por sus siglas en inglés*)* y, con ello, la desaprobación de gran parte de la comunidad internacional. El sistema informático que les habría facilitado a las autoridades represivas ejecutar esta vigilancia masiva se denominó "PRISM", lo que les permitía *"captar correos electrónicos, videos, fotografías, llamadas de voz y de imagen, actividad en los medios sociales, contraseñas y otros datos de usuarios contenidos por las principales empresas de internet en EEUU"* [7].

Por su parte, en julio de 2015, poco tiempo después de los atentados de París, Francia votó una legislación "antiterrorista" en la que, sin la necesaria exigencia de una orden jurisdiccional, se obliga a las empresas proveedoras de los servicios telefónicos e Internet a instalar "cajas negras" que proporcionen masivamente datos telefónicos y de Internet de las personas usuarias,

6 *Accedido el 2/14/2019* https://www.justice.gov/archive/ll/highligths.htm

7 *Márquez William. "Lo que Snowden ha revelado hasta ahora del espionaje de EE.UU". Diario BBC Mundo (Washington, 7/02/2013), página web* www.bbc.com/ *accedido el 7/02/19*

Volver al índice

bajo la mampara de la protección de los intereses económicos, políticos o la seguridad nacional.

Amnistía Internacional acotó sobre el particular que:

> *esta ley viola flagrantemente los derechos humanos internacionales a la intimidad y a la libertad de expresión. Cualquier persona que investigase las actividades del gobierno francés o de una empresa francesa, o que organizara siquiera una protesta, podría ser sometida a formas de vigilancia muy intrusivas. Las herramientas de vigilancia masiva como las cajas negras, pondrían las comunicaciones por internet de toda la población y más allá al alcance de las autoridades francesas*[8].

Ahora bien, dando por entendido que las grandes empresas multinacionales propietarias de RRSS y *Apps* de mensajería rápida muestran una actitud reacia hacia la *interceptación de comunicaciones digitales* de personas sospechosas del crimen organizado, nos preguntamos: ¿con base en lo dispuesto en el Convenio de Budapest, podrían impulsarse acciones legislativas tendientes a la instalación de *software* que permita la vigilancia de datos electrónicos con la debida supervisión jurisdiccional? ¿Pueden los órganos de policía tener acceso a algunos de estos datos que les permita conocer al menos perfiles en redes sociales (de acceso privado), actividades cotidianas y vínculos sociales –por mencionar algunos- que les facilite la conformación de un perfil criminal? Si esto es una realidad, ¿tienen nuestros países la capacidad financiera y estructural para el análisis en tiempo real de miles o decenas de miles de mensajes de texto, audios, videos, entre otros que hagan funcional y operativa la labor policial en pleno resguardo de las garantías fundamentales de los mismos intervenidos y del resto de la ciudadanía?

V. El caso de AUSTRALIA: ¿acierto o legislación intrusiva?

El 16 de diciembre de 2018, el Parlamento australiano aprobó la llamada "Ley de Asistencia y Acceso a las Comunicaciones" o "Ley Anticifrado" que obliga a las empresas administradoras de redes sociales, incluyendo *Apple, Facebook y Whatsapp,* crear en sus plataformas de seguridad de mensajería dispositivos conocidos como *backdoors* (puertas traseras) que tienen como fin descifrar los mecanismos de encriptación para acceder a las comunicaciones.

La ley incluye la potestad de obligar a las personas encargadas de Tecnologías de Información (TI) a ejecutar acciones tendientes a *debilitar* la seguridad de estos sistemas bajo pena de multa a las empresas y de privación de libertad a sus empleados[9]. Los "niveles de asistencia" que se regulan son tres: a) asistencia a las autoridades policiales mediante la eliminación de la protección electrónica, instalación de *software* y facilitar acceso a dispositivos o servicios; b) interceptación de las comunicaciones sin mayor trámite cuando no exista cifrado y c) la obligatoriedad de las empresas de desarrollar "nuevas capacidades" para descifrar las comunicaciones que requiera la Policía[10].

8 *Amnistía Internacional. "Francia: nueva ley de vigilancia, duro golpe para los derechos humanos", página web* www.amnesty.org/ *accedido el 7/20/2019*

9 *Tarabay, Jaime. "Australian Government Passes Contentious Encryption Law". Diario The New York Times (Nueva York, 12/06/2018), página web https://www.nytimes.com/accesado el 7/22/19*

10 *Accedido el 07/23/2019 https://noticiasseguridad.com*

Volver al índice

Las críticas no se hicieron esperar, no solo en lo concerniente a la vulneración de prerrogativas fundamentales, sino también respecto a la franca desproporcionalidad de las sanciones previstas en caso de omisión. Pero además se estima que crear "puertas abiertas" implicaría un grave riesgo no solo para este país, sino también para el resto del mundo, dada la naturaleza *trasnacional* de la web.

En nuestra opinión, aunque se reconoce la importancia de la vigilancia electrónica del crimen organizado para la investigación de delitos graves, desde la óptica jurídica y técnica, esta legislación incluye importantes desaciertos que deben ser advertidos: técnicamente, parece que los legisladores no se apoyaron en un estudio serio que examinara a profundidad las consecuencias derivadas del debilitamiento de los sistemas de encriptación para la totalidad de las personas usuarias. Se ha asumido que la red es una para todos, por lo que la creación de *backdoors* facilitaría que los mismos *hackers* puedan ingresar a esos sistemas y cometer otros delitos informáticos.

Otro de los problemas que se avizora tiene que ver con la *logística, personal e infraestructura* que se emplearán para la *interceptación en tiempo real* de las comunicaciones en redes sociales y aplicaciones de mensajería rápida. Aunque no se aprecia problema alguno para el decomiso y entrega de evidencia *ex post facto* (entrega formal de datos almacenados), queda la duda de cómo se evaluarán las decenas de miles de datos digitales que ingresarán día a día sin comprometer la privacidad de las personas usuarias de los servicios u otras prerrogativas como el derecho de defensa.

Cabe recordar que Costa Rica cuenta con una dependencia de carácter eminentemente jurisdiccional (CJIC) para realizar esta labor (actualmente, comunicaciones telefónicas) con ajenidad total de la participación de empresas proveedoras.

Por su parte, en lo conducente a los desaciertos de orden jurídico, la ley otorga facultades absolutas para el manejo de estos datos en los órganos de policía, relevando, con ello, toda supervisión jurisdiccional.

Debe recordarse que al tenor del numeral 24 constitucional patrio, la intervención de comunicaciones será ordenada por los tribunales de la república bajo la estricta vigilancia y responsabilidad indelegable de las personas juzgadoras, lo que supone mayores garantías para las personas intervenidas y demás participantes no involucrados en las pesquisas. No debe echarse de menos la prohibición legal del párrafo segundo del artículo 26 de la Ley 7425 para la inclusión dentro del legajo de intervención de aquellas comunicaciones orales o escritas –y por supuesto, digitales- que ocurran entre el intervenido y su patrocinio letrado debidamente acreditado con ocasión de su derecho de defensa.

En esta misma línea, la "Ley Anticifrado" no estimó qué sucede cuando en una comunicación de este tipo, la persona defensora sugiere a la persona intervenida la comisión de hechos delictivos o contravencionales como parte de su estrategia de defensa. Difícilmente, las empresas proveedoras del servicio o aun las autoridades policiales de Australia harán las necesarias valoraciones jurídicas de previo a la correcta selección de los correos electrónicos o los datos de *Whatsapp, Messenger* o similares que serán lícitamente incorporados.

Por otro lado, consideramos absolutamente desproporcionadas las sanciones privativas de libertad contra los empleados de tecnología de información que, por una u otra razón de orden técnico, de seguridad cibernética o aún jurídicas, estos no puedan o no deban atender los

Volver al índice

requerimientos policiales. Bajo esta tesitura, nos cuestionamos: ¿hasta dónde debe llegar ese deber de asistencia policial? ¿Ante qué instancia podrían los proveedores de los servicios acudir en caso de discordancias de orden técnico? ¿En cuáles conductas típicas podrían incurrir los servidores de TI, si se niegan "a colaborar"? ¿Qué negativas podrían más bien representar verdaderas causas de justificación u obediencia debida?

VI. Una propuesta para Costa Rica

El empleo de redes sociales, correos electrónicos y aplicaciones de mensajería rápida por parte de la delincuencia organizada común y los y las cibercriminales es una realidad cada vez más acentuada en nuestro país. El acceso casi ilimitado a la información que proporciona la Internet les ha permitido conocer las prerrogativas de la utilización de dichas herramientas tecnológicas frente a otros medios convencionales –y prácticamente desfasados- de comunicación. Esto deja en franca desventaja la oportuna acción policial, la cual urge de un robusto sistema jurídico que le otorgue *igualdad de armas* para combatir más eficientemente estos flagelos.

De esta manera, creemos que la tarea de vigilancia electrónica en delitos graves y organizados es una necesidad en la realidad jurídica y social costarricenses. El Convenio de Budapest de 2001 debe servir como normativa marco para el inicio de la producción legislativa interna que sea efectiva y no simbólica; pero también lo menos intrusiva posible. En sus numerales 20 y 21, a nuestro juicio, se reglan las herramientas necesarias para el inicio de lo que será un cambio de paradigma en la investigación de los hechos delictivos que más aquejan a nuestra sociedad en la era digital.

Para ello, el producto legislativo que emane de nuestro Congreso deberá aprender de las experiencias erráticas de países como Estados Unidos, Francia o Australia y deberá materializar un justo balance entre la necesidad de dotar a la Policía y al Ministerio Público de verdaderas herramientas de investigación y de recopilación de pruebas legítimas; pero sin dejar vacíos de contenido los alcances del canon 24 constitucional.

En este orden, quisiéramos presentar los siguientes apuntes a modo de recomendación:

a) Deben reformarse la Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones, N.º 7425 del 9 de agosto de 1994, así como la Ley contra la Delincuencia Organizada, N.° 8754 del 24 de julio de 2009, de tal manera que puedan adaptarse ambos textos a la nueva realidad que imponen los numerales 20 y 21 del Convenio de Budapest. De previo, debe contarse con un estudio técnico de alto nivel que determine las reales capacidades de las empresas proveedoras de servicio locales y transnacionales para una efectiva *interceptación en tiempo real de las comunicaciones electrónicas.* Este análisis debe incluir, entre otras variables, las desventajas de abrir *backdoors* para la seguridad y privacidad cibernéticas del resto de las personas usuarias.

b) Excluir de toda consideración, la posibilidad de instalación de *troyanos, keyloggers* o cualquier otro tipo de *malware* que implique vigilancias masivas en la red.

c) Toda la labor de supervisión y vigilancia del material digital (mensajes de texto, videos, imágenes, audios) será resorte exclusivo del Centro Judicial de Intervención de las Comunicaciones (CJIC), ente que deberá ser dotado de los recursos tecnológicos y humanos necesarios para ejecutar con notable eficiencia dichas funciones.

Volver al índice

d) Facultar al Ministerio Público y a la Policía judicial para que estos tengan acceso a los "datos de tráfico" que no involucren contenido sensible ni privado, y que estas entidades puedan compartirlas con sus homólogos de otros países cuando la actividad delictiva sea transfronteriza.

e) Las reformas deben enunciar sin ambages las "obligaciones y responsabilidades" de cada proveedor de servicios imponiendo sanciones pecuniarias para la empresa y no privativas de libertad para sus servidores (responsabilidad civil objetiva y no personalísima de prisión), incluyendo las instancias nacionales e internacionales encargadas de dirimir los conflictos que se presenten.

f) Las reformas que se promuevan deberán observar *en lo que sea posible de acuerdo con nuestro derecho interno* los **Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones,** documento impulsado por la ONG ***"Necessary & Proporcionate"*** y lanzado por el Consejo de Derechos Humanos de la ONU en septiembre de 2013[11].

1) Principio de legalidad: Toda intrusión al derecho fundamental a la privacidad debe emanar de una ley previa y clara, y sus reformas deben atender el ritmo de los avances tecnológicos.

2) Objetivo legítimo: Las personas intervenidas deben responder a objetivos legítimos según un interés democrático preponderante, con ajenidad de cualquier consideración sobre raza, color, sexo, religión, posición económica y otros.

3) Necesidad: La vigilancia de las comunicaciones debe ejecutarse cuando es el único medio para alcanzar objetivos legítimos o, cuando habiendo varios, sea el menos lesivo de derechos de primer orden.

4) Idoneidad: La vigilancia autorizada debe ser adecuada para cumplir el objetivo legítimo específico.

5) Proporcionalidad: La intervención en las comunicaciones debe ser considerada altamente intrusiva por lo que debe ser proporcional a la gravedad de los hechos que se pesquisan ponderando intereses legítimos de mayor prevalencia.

6) Autoridad judicial competente: Todo lo concerniente a la vigilancia de las comunicaciones será resorte de los tribunales de la república como ente objetivo e imparcial, por lo que deberá estar separada (funcionalmente) de los órganos de investigación y capacitada técnica y logísticamente para llevar a cabo esas tareas.

7) Debido proceso: Los Estados deberán prever mecanismos procesales justos, objetivos y accesibles (audiencias orales, recursos impugnatorios) que garanticen un adecuado ejercicio de defensa de las personas intervenidas en caso de vulneración de máximas fundamentales.

8) Notificación a la persona usuaria: La persona usuaria debe ser notificada de la acción de la vigilancia salvo que este conocimiento previo comprometa la finalidad por la que se autoriza la

11 Accedido el 07/23/2019, https://necessaryandproporcionate.org/es/

Volver al índice

interceptación o se ponga en serio peligro la vida humana.

9) **Transparencia:** Las actuaciones del Estado en torno a la vigilancia de las comunicaciones debe ser pública con estadísticas que incluyan número de solicitudes aprobadas y rechazadas, desglose de las gestiones por proveedor y por autoridad solicitante, el tipo de investigación y propósito, entre otras variables.

10) **Supervisión pública:** Los Estados deben contemplar en sus legislaciones la rendición de cuentas ante un órgano distinto al Gobierno que garantice la transparencia y legitimidad de sus actuaciones.

11) **Integridad de las comunicaciones y sistemas:** Los Estados no deben exigir a los proveedores de los servicios desarrollar por ellos mismos la capacidad de vigilancia o de control en sus sistemas, sino que serán aquellos los que provean esas herramientas.

12) **Garantías para la cooperación internacional:** En la dinámica de asistencia judicial recíproca, cuando varias legislaciones resulten aplicables a varios Estados, deberá optarse por la alternativa estándar que mejor garantice la protección de las personas. Así mismo, deberá constatarse la aplicación del *principio de doble incriminación*[12] cuando un Estado pretenda hacer cumplir su legislación interna.

13) **Garantías contra el acceso ilegítimo y derecho a recurso efectivo:** Estas incluyen el deber de los Estados de sancionar punitivamente los accesos ilegales a las plataformas digitales, los mecanismos procesales de reparación civil a las personas afectadas, la declaratoria de invalidez de las pruebas obtenidas por medios distintos a los legalmente estatuidos así como la destrucción o devolución a su legítimo titular de las evidencias decomisadas cuando no proceda el comiso.

CONCLUSIÓN

El uso inescrupuloso por parte del crimen organizado de medios electrónicos para la comisión de *ciberdelitos* o como vehículo logístico para materializar otros ilícitos graves transnacionales es una realidad cada vez más acentuada en nuestra sociedad. Las prerrogativas que la web les brinda a estos grupos los coloca en una posición ventajosa dados los caracteres de agilidad, gratuidad y anonimato que caracterizan a las redes sociales y aplicaciones de mensajería rápida, frustrando así la oportuna acción policial. Por esto, la vigilancia electrónica de las comunicaciones *en tiempo real* es una necesidad que debe implementarse con la mayor brevedad.

La Ley N.º 7425 del 9 de agosto de 1994, Ley de Registro, Secuestro de Documentos e Intervención de las Comunicaciones y la Ley N.° 8754 del 24 de julio de 2009, Ley contra la Delincuencia Organizada, son insuficientes para lograr este cambio de paradigma, por lo que ambas deben ser reformadas delimitando con claridad las acciones, facultades, procedimientos

12 *El principio de doble incriminación exige que las conductas delictivas que justifiquen una extradición deben estar debidamente incorporadas en las normativas internas de cada país, mediante una ley pública y previa. Aplicado al tema en cuestión, debe entenderse que cuando se pretenda justificar la interceptación de comunicaciones por delitos transfronterizos, las conductas típicas que motivan este acto intrusivo deben estar contempladas en todos los países involucrados en la investigación internacional.*

Volver al índice

y solución de controversias que permitan compeler a las empresas proveedoras de servicios de estos sistemas de tráfico de datos, tomando como base las Reglas del Convenio de Budapest sobre Delincuencia de 2001, ratificado por Costa Rica desde el 2017.

Esta tarea de vigilancia y supervisión de datos digitales privados deberá ser competencia exclusiva del Centro Judicial de Interceptación de las Comunicaciones como ente de carácter jurisdiccional, objetivo e imparcial que garantice a las personas intervenidas y al resto de personas usuarias del ciberespacio, la efectiva tutela de sus derechos fundamentales.

REFERENCIAS BIBLIOGRÁFICAS

Amnistía Internacional. "Francia: nueva ley de vigilancia, duro golpe para los derechos humanos", accedido el 7/20/2019, página web www.amnesty.org/2015/07Francia: Nueva ley de vigilancia, duro golpe para los derechos humanos

Convenio de Budapest sobre Ciberdelincuencia de 2001, accedido mediante http://pgrweb.go.cr, el 2/13/2019.

Constitución Política de la República de Costa Rica, accedida mediante http://pgrweb.go.cr, el 2/13/2019.

Departamento de Justicia de los Estados Unidos, "The USA Patriot Act: Preserving Life and Liberty", accedido el 2/14/2019, *https://www.justice.gov/archive/ll/highligths.htm*

Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones N.º 7425 del 9 de agosto de 1994, accedida mediante http://pgrweb.go.cr, el 2/13/2019.

Ley 8754 del 24 de julio de 2009, Ley contra la Delincuencia Organizada, accedida mediante http://pgrweb.go.cr, el 2/13/2019

Márquez William. "Lo que Snowden ha revelado hasta ahora del espionaje de EE.UU". *Diario BBC Mundo* (Washington), accedido el 7/02/2019, página web www.bbc.com/Lo que Snowden ha revelado hasta ahora del espionaje de EE.UU – BBC News

Sin autor. "¿Por qué Brasil se quedó sin WhatsApp por orden judicial?". *Diario BBC Mundo* (Nueva York), accedido el 7/19/2019, página web www.bbc.com/Por qué Brasil se quedó sin Whatsapp por orden judicial-BBC News Mundo

Suárez Eduardo. "Facebook compra WhatsApp por 19.000 millones de dólares". *Diario El Mundo* (Nueva York), accedido el 7/20/2019, https://www.elmundo.es/2014/10/07Facebook compra WhatsApp por cerca de 17.000 millones de euros

Tarabay, Jaime. "Australian Government Passes Contentious Encryption Law". *Diario The New York Times* (Nueva York), accedido el 7/22/2019, https://www.nytimes.com/Australian Government Passes Contentious Encryption Law-The New York Times
https://noticiasseguridad.com/ley-anticifrado es aprobada en Australia-Noticias de Seguridad, accedida el 7/22/2019.

https://necessaryandproporcionate.org/es/necesarios-proporcionados, accedida el 7/23/2019,

Volver al índice