lavits ****** 2017
5to Simposio Internacional LAVITS
Vigilancia, Democracia y Privacidad
en América Latina: Vulnerabilidades y resistencias

ISSN 2175-9596

CONFLICTOS DE SOBERANÍA EN LA IMPLEMENTACIÓN DEL CONVENIO DE BUDAPEST: ANÁLISIS CRÍTICO DE LA CONSERVACIÓN Y ACCESO TRANSFRONTERIZO DE DATOS PERSONALES PARA LA PERSECUCIÓN INTERNACIONAL DE CIBERDELITOS

Conflitos de soberania na implementação da Convenção de Budapeste: análise crítica da conservação e acesso transfronteiriço de dados pessoais para a perseguição internacional de cibercrimes

Conflicts of sovereignty in the implementation of the Budapest Convention: critical analysis of the conservation and cross-border access of personal data for the international persecution of cybercrimes

Eduardo Estrada Aravena[a]

[(a)] Abogado – Universidad de Chile. Diplomado en Ciberseguridad y Ciberdefensa – Universidad de Chile. Actualmente cursando el 73° Programa de Formación de la Academia Judicial. E-mail: eestrada@ug.uchile.cl

Resumen

La polémica suscitada en Chile por la divulgación del decreto promovido por el Gobierno para establecer un sistema permanente de conservación de datos de comunicación y geolocalización de las personas, con el pretexto de actualizar el actual reglamento de interceptaciones telefónicas y mejorar los mecanismos de persecución penal; ha sido tratada desde las organizaciones sociales como un intento por instaurar un Estado de Vigilancia vulneratorio de las garantías consagradas por nuestra Constitución Política, excediendo los límites de la potestad reglamentaria, pues la inviolabilidad de toda comunicación privada corresponde a una materia de exclusivo dominio legal. Sin embargo, por parte del Gobierno se argumenta la necesidad de actualizar el actual reglamento para permitir a los órganos de la administración de justicia el acceso oportuno a una información ya almacenada por las empresas de telecomunicaciones con fines comerciales. En el presente trabajo analizaremos no la ilegalidad del medio empleado para la modificación, sino más bien los peligros que conllevaría su regulación por vía legislativa, en cumplimiento de un

compromiso que el Estado ya asumió al ratificar el Convenio de Budapest que, especialmente en su artículo 32, establece la necesidad de adaptar la legislación nacional para permitir el acceso transfronterizo a datos personales sensibles de la población, incluso sin autorización, con el propósito de combatir el cibercrimen. En particular, trataremos la amenaza que ello supone a nuestra soberanía, ponderando la discusión doctrinaria entre vigilancia y ciberdefensa.
Palabras clave: Soberanía; Vigilancia; Datos personales; Acceso transfronterizo; Ciberdelitos.

Resumo

A controvérsia levantada no Chile para a divulgação do decreto promovido pelo Governo para estabelecer um sistema permanente de conservação de dados de comunicação e geolocalização de pessoas, com pretexto de atualizar os atuais regulamentos sobre interceptações telefônicas e melhorar os mecanismos de perseguição criminal; foi tratado pelas organizações sociais como uma tentativa de estabelecer um Estado de Vigilância que viole as garantias consagradas em nossa Constituição Política, superando os limites do poder regulador, uma vez que a inviolabilidade de toda comunicação privada corresponde a uma questão de controle legal exclusivo. No entanto, o Governo argumenta a necessidade de atualizar o atual regulamento para permitir que os órgãos da administração de justiça tenham acesso oportuno a informações já armazenadas por empresas de telecomunicações para fins comerciais. No presente trabalho, analisaremos não a ilegalidade dos meios utilizados para a modificação, mas sim os perigos que sua regulamentação por meios legislativos implicariam, em cumprimento de um compromisso que o Estado já assumiu ao ratificar a Convenção de Budapeste, especialmente em seu artigo 32, estabelece a necessidade de adaptar a legislação nacional para permitir o acesso transfronteiriço a dados pessoais sensíveis da população, mesmo sem autorização, com o objetivo de combater o cibercrime. Em particular, abordaremos a ameaça que isso representa para nossa soberania, ponderando a discussão doutrinária entre vigilância e ciberdefensa.
Palavras-chave: *Soberania; Vigilância; Dados pessoais; Acesso transfronteiriço; Cibercrimes.*

Abstract

The controversy raised in Chile for the disclosure of the decree promoted by the Government to establish a permanent system of conservation of communication data and geolocation of people, under the pretext of updating the current regulations on telephone interceptions and improving the mechanisms of criminal prosecution; it has been treated by social organizations as an attempt to establish a State of Vigilance that violates the guarantees enshrined in our Political Constitution, exceeding the limits of the regulatory power, since the inviolability of all private communication corresponds to a matter of exclusive legal control. However, the Government argues the need to update the current regulation to allow the organs of the administration of justice timely access to information already stored by telecommunications companies for commercial purposes. In the present work we will analyze not the illegality of the means used for the modification, but rather the dangers that its regulation by legislative means would entail, in fulfillment of a commitment that the State already assumed when ratifying the Budapest Convention, especially in its article 32, establishes the need to adapt national legislation to allow cross-border access to sensitive personal data of the population, even without authorization, for the purpose of combating cybercrime. In particular, we will address the threat that this poses to our sovereignty, pondering the doctrinal discussion between surveillance and cyberdefense.
Keywords: *Sovereignty; Surveillance; Personal data; Cross-border access; Cybercrime.*

INTRODUCCIÓN: TODOS (SABEMOS QUE NOS) ESPÍAN

Casi toda nuestra actividad en la Red deja algún tipo de rastro, al menos desde que los dueños de los predios digitales que visitamos descubrieran la utilidad de estas huellas -o caminos ya recorridos- para la generación de nuevos servicios, o bien, para el refinamiento de los principales productos ofrecidos. Aceptamos con indiferencia – sin siquiera revisar – las condiciones de servicio y las políticas de privacidad de las aplicaciones móviles o web que utilizamos a diario, principalmente por razones de oportunidad; por resultar una condición para acceder a la tecnología que nos sugiere canciones relacionadas con nuestras preferencias, o geolocalizar nuestra ubicación para ofrecernos un taxi o nuestra comida favorita.

El cinismo que nos motiva, se ve claramente reflejado en la ambivalencia con que los usuarios tratamos el tema de nuestros datos personales. Aun cuando las corporaciones internacionales como Facebook o Google mantienen una cantidad de usuarios activos que supera largamente la cantidad de ciudadanos de un Estado promedio; pareciera que sólo cuando un Estado desarrolla actividades para el tratamiento de nuestra información despierta en nosotros una voz de alarma para defender nuestra privacidad en contra de una vigilancia masiva.

Lo anterior, en circunstancias que, por definición, es el Estado quien debiese defendernos de las amenazas que podemos encontrar en la Red y perseguir a los responsables de delitos comunes que toman los medios digitales como formas de comisión, o delitos que sólo pueden ejecutarse por esta vía, como resultan los informáticos o ciberdelitos. Como existe una asimetría de conocimientos técnicos entre los usuarios comunes y los programadores de las páginas que visitamos, y en la medida que esta brecha se acrecienta ante un ciberdelincuente, o un espía informático; correspondería que el Estado tutele los derechos fundamentales que pueden ser afectados a sus ciudadanos en la Red, con los recursos y atribuciones que detenta, cuando las medidas de autoprotección no resultan suficientes.

Sin embargo, no sólo nos encontramos expuestos los usuarios a los distintos ataques y anzuelos dispuestos en la Red, sino también los propios Estados ven amenazada la Seguridad Nacional y la estabilidad de sus instituciones que, por cierto, conservan una gran cantidad de datos personales. Ciberataques como el sufrido por Estonia en 2007 en el incidente de Tallin, así como el detectado en el Parlamento Alemán en 2015, han motivado que distintos gobiernos del mundo contraten

especialistas en seguridad de la información que permitan proteger sus sistemas del espionaje y sabotaje foráneos, así como estar preparados para responder rápidamente a un incidente de estas características.

Asimismo, los ataques terroristas dirigidos contra la población civil en las principales ciudades y capitales de Europa en lo que va del año 2017, como la explosión en el concierto de Ariana Grande en Manchester, y las furgonetas que arroyaron en Londres y Barcelona a miles de turistas, cobrando decenas de vidas; han hecho renacer el debate público acerca de las herramientas que puede utilizar el Estado para prever y prevenir este tipo de ataques, interviniendo las comunicaciones y bajo qué costo, en lo que respecta a la limitación o restricción de garantías fundamentales de sus ciudadanos.

En la medida que el ciberespacio permite a los atacantes traspasar fronteras y ocultar sus huellas en la Red (puesto que poseen una capacidad técnica superior al usuario promedio), se hace necesario que los Estados desarrollen herramientas de apoyo a la persecución penal que sean acordes a este tipo de delitos o actos preparatorios. También resulta fundamental que se establezcan mecanismos de cooperación internacional que favorezcan un actuar oportuno entre Estados, con el fin de evitar que las investigaciones se estanquen en proceso burocráticos que devienen en la impunidad de estas conductas transfronterizas.

DECRETO 866 EN RELACIÓN AL CONVENIO DE BUDAPEST

Inscrita en este problema global, se encuentra la entrada en vigencia en Chile del Convenio sobre Ciberdelincuencia del Consejo de Europa, conocido también como el Convenio de Budapest[1], desde agosto del presente año 2017; que implicará una serie de acciones para comprometer la participación de organismos públicos y privados con el objetivo de promover un *"ciberespacio libre, abierto, seguro y resiliente"*[2].

Hasta el momento, la más polémica de ellas consiste en el denominado "decreto espía" (decreto

[1] Disponible en español en: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c. Recuperado el 30 de octubre de 2017.
[2] Política Nacional de Ciberseguridad. Disponible en: http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf. Recuperado el 30 de octubre de 2017.

N°866[3]) del Ministerio del Interior y Seguridad Pública, que actualmente se encuentra en proceso de toma de razón en la Contraloría General de la República y que pretende *"introducir mejoras al actual procedimiento de interceptaciones"*.

La principal crítica de las organizaciones civiles consiste en que el gobierno pretende regular por vía reglamentaria una materia sobre la que existe estricta reserva legal, con el pretexto de la entrada en vigencia del Convenio de Budapest. Sin embargo, pocos han dirigido sus observaciones a lo sustantivo. Nos parece que la discusión importante tiene que ver más con el caso en que, superado el punto sobre la forma, el gobierno regule la materia a través de una ley.

ACTUALIZANDO NUESTRA LESGISLACIÓN

El Convenio de Budapest tiene como principales objetivos: i) armonizar los elementos sustantivos de la legislación penal relacionada con disposiciones del cibercrimen; ii) ofrecer las facultades necesarias sobre derecho procedimental doméstico para la investigación y persecución de delitos y otras conductas cometidas a través de sistemas de cómputo y para la obtención de pruebas en relación a la información contenida en forma electrónica; y iii) establecer un régimen ágil y efectivo de cooperación internacional, entre otros objetivos.

La necesaria reforma de la legislación interna, consiste entonces en el principal compromiso adoptado por cada uno de los Estados signatarios en orden a implementar las medidas sugeridas por el Comité de Expertos en Ciberespacio; como puede apreciarse en la gran mayoría de los artículos que componen la Convención: *"adoptar las medidas legislativas y de otro tipo que resulten necesarias para…"*.

Sin embargo, la tipificación de nuevos delitos, procedimientos, mecanismos de cooperación internacional y facultades de las autoridades establecidas en el Convenio de Budapest deberán sujetarse a un marco mínimo de derechos, así como al principio de proporcionalidad, tal como señala el artículo 15:

[3] Documento disponible en: https://www.derechosdigitales.org/wp-content/uploads/decreto-866-2017.pdf. Recuperado el 30 de octubre de 2017.

> Artículo 15 - Condiciones y salvaguardas.
> Cada Parte se asegurará de que el establecimiento, la ejecución y la aplicación de los poderes y procedimientos previstos en la presente sección **están sujetas a las condiciones y salvaguardas previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades**, incluidos los derechos derivados de las obligaciones asumidas en virtud del Convenio del Consejo de Europa para la protección de los derechos humanos y las libertades fundamentales (1950), del Pacto Internacional de derechos civiles y políticos de las Naciones Unidas (1966), y de otros instrumentos internacionales aplicables en materia de derechos humanos, y que **deberá integrar el principio de proporcionalidad.**
> Cuando resulte procedente dada la naturaleza del procedimiento o del poder de que se trate, **dichas condiciones incluirán, entre otros aspectos, la supervisión judicial u otra forma de supervisión independiente, los motivos que justifiquen la aplicación, y la limitación del ámbito de aplicación y de la duración del poder o del procedimiento de que se trate.**
> Siempre que sea conforme con el interés público y, en particular, con la correcta administración de la justicia, cada Parte examinará la repercusión de los poderes y procedimientos previstos en la presente sección en los derechos, responsabilidades e intereses legítimos de terceros (grifos del autor).

De esta forma, todas las medidas deben inscribirse necesariamente desde una perspectiva de respeto por los derechos humanos y garantías, como resulta en nuestro país la establecida en el artículo 19 N°5 de nuestra Constitución Política, esto es, la inviolabilidad del hogar y de toda forma de comunicación privada, que sólo puede ser restringida por ley.

En lo que respecta a la conservación de datos, el Convenio de Budapest establece, primero, dos definiciones para diversos tipos de datos:

> **Datos informáticos:** cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático.
> **Datos sobre el tráfico:** cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente.

Respecto a los datos informáticos, en los que puede encasillarse prácticamente cualquier dato personal, el artículo 16 establece la necesidad de implementar potestades para que la autoridad competente pueda imponer su conservación rápida a quien se encuentra bajo su control, por un tiempo máximo de 90 días y con el fin específico de conseguir su revelación. Por su parte, con el fin de garantizar la conservación de los datos de tráfico, exclusivamente, el artículo 17 señala las medidas para identificar a los proveedores de servicio y la vía por la que se transmitió la comunicación.

Puede adelantarse que, en modo alguno, los artículos citados hacen referencia a la necesidad de mantener un registro que conserve en forma preventiva los datos informáticos de todas las personas, sino de facultades para permitir a la autoridad su revelación, en caso que una persona o prestador de servicios se encuentre en posesión de dichos datos; lo que en nuestra legislación correspondería, según la ley N°19.628 sobre protección de la vida privada, al responsable del registro o banco de datos, como señala el artículo 2 letra n) de dicho cuerpo legal.

CONSERVACIÓN DE DATOS COMO MEDIDA CONTINGENTE Y LIMITADA

Como señaláramos, si bien en este punto ya puede advertirse la imposibilidad de regular por vía reglamentaria una materia en la que nuestra Constitución dispone expresamente su reserva legal; nos parece que la discusión importante tiene que ver más con el caso en que, superado el punto sobre la forma de la modificación, el Gobierno emprenda el camino adecuado y regule lo mismo que pretendió por medio del decreto en discusión, esta vez por vía de una ley.

De esta manera, analizando ya propiamente el decreto 866, podemos señalar que se regulan principalmente dos materias. La primera, referida propiamente a una actualización del reglamento sobre intercepción de comunicaciones y, la segunda, innovando sobre la conservación -por parte de los prestadores de servicios de telecomunicaciones- no solo de datos de tráfico, como hace referencia el artículo 222 del Código Procesal Penal; sino otros datos personales, como resultan la identidad de los usuarios, su ubicación geográfica y "cualquier otra información que una norma técnica les exija".

Respecto a la primera materia, señala el inciso 5° del referido artículo 222 del CPP que lo que debe mantenerse a disposición del Ministerio Público, exclusivamente, es 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 realicen sus abonados. Puede advertirse que la *ratio iuris* de la norma, corresponde a la mantener un registro para que, en caso que sea autorizada la medida intrusiva, pueda identificarse el equipo que será intervenido en relación al número de IP de la conexión utilizada por el abonado. Identificado el objeto de la interceptación, comenzarán a registrarse los datos de voz u otro tipo de comunicaciones a contar de la fecha de la respectiva autorización judicial.

En ningún caso la norma señala que el objeto de la revelación sea el listado o el número de IP mismo,

sino sólo corresponde a una identificación para hacer efectiva la medida; razón por la cual aplicar por analogía cualquier otro tipo de datos, por decirlo así, sustantivos, excede el mandato legal. De hecho, en nuestro país existe un efectivo control judicial respecto a la resolución motivada que autoriza este tipo de intercepciones, toda vez que la defensa puede cuestionar los fundamentos, oportunidad y duración de la medida, llegando incluso al extremo de ser excluida toda la prueba derivada de una intercepción autorizada judicialmente, pero que resultó ilegal en su ejecución o no ser efectivos sus fundamentos (Alvarado, 2014).

Si las fundadas sospechas tenidas en consideración para la autorización de la medida intrusiva, se disipan o hubiere transcurrido su plazo concedido, ésta debe ser dejada sin efecto inmediatamente, atendido su carácter instrumental y la aplicación de la regla *rebus sic stantibus*, conforme a la cual solo debe mantenerse mientras subsista el fundamento que la hizo procedente (Alvarado, 2014).

Ese es el criterio que también ha adoptado nuestra jurisprudencia:

> **ROL 3016/2011 CORTE SUPREMA:** De todo lo expresado se colige que, es cierto que la Policía de Investigaciones realizó una interceptación telefónica al margen de la ley, violentando de manera expresa el artículo 222 del Código Procesal Penal que faculta dicha intervención, sólo con beneplácito del juez, en los supuestos que se verifiquen las coyunturas que esa misma norma señala. El resultado de esa ilegítima actuación, no podía ser presentado como medio de prueba en el procedimiento, tal como lo prescribe el artículo 225 del ordenamiento del ramo.

De esta forma, en lo relativo a la materia de conservación y revelación de datos personales por parte de las empresas de telecomunicaciones, en caso de modificarse la redacción del inciso 5° del artículo 222 del CPP para incluirlos, consideramos que debe revisarse lo indicado en el apartado 2° del artículo 15 del Convenio de Budapest, en el sentido de exigirse la supervisión judicial de una medida que necesariamente debe regir para el futuro, en razón del principio de proporcionalidad. Como se puede advertir, ciertamente no puede resultar proporcional mantener a toda la población vigilada a cambio de mejores herramientas de combate a la cibercriminalidad.

Sostendremos que la autoridad competente – en los términos de lo indicado en los artículos 16 y 17 del Convenio- para ordenar la conservación de datos, corresponde a un juez de garantía, para una investigación penal en curso, bajo estrictas condiciones de admisibilidad, a contar de la fecha de la

resolución y durante un plazo determinado.

Que el Gobierno de Chile interprete dichas disposiciones en el sentido que la autoridad competente resultaría el ministerio del ramo y que lo ordenado sea la creación de un registro permanente para mantener almacenados los datos de toda la población, para que el órgano persecutor pueda acceder a ellos si un juez lo autoriza; resulta una doble equivocación. Primero, invoca el Convenio de Budapest cuanto dicho tratado no recomienda tal registro sino el acceso a la revelación de datos. Además, interpreta erróneamente el sentido de lo dispuesto en el artículo 222 del CPP, que se refiere al listado de rangos y números de IP, sólo para identificar el objeto de una medida intrusiva que regirá para el futuro.

Ese error resulta manifiesto en la redacción del artículo 12° del mencionado decreto 866 que establece un nuevo tipo de diligencia de investigación que puede solicitar el fiscal al juez de garantía competente, y que corresponde a una aparente reproducción de la recomendación establecida en el artículo 16 del Convenio de Budapest. De ponerse en práctica el decreto, o incluirse esta diligencia en una modificación legal al artículo 222 del CPP, traería como consecuencia una medida impracticable pues no se indica, en términos técnicos, cómo una persona no especialista, incluso el propio imputado, pueda proteger los datos comunicacionales, qué sanciones acarrea el incumplimiento, en que consiste la prórroga, cómo afecta la prohibición de autoincriminación, etc.

En consecuencia, aun cuando el mencionado decreto se transformara en una ley de “agenda corta” para la cibervigilancia; tal proyecto tendría que hacerse cargo de la discusión sobre la proporcionalidad de una medida preventiva, de la necesidad de autorización judicial previa, por cuánto tiempo, bajo qué antecedentes, etc. Afortunadamente, existen ejemplos en el Derecho comparado que nos pueden dar algunas luces.

BAREMOS PARA LA INTERCEPTACIÓN

Superada la discusión acerca de si es legal o no regular esta materia mediante un decreto (por supuesto que no lo es), corresponde preguntarnos si podría ser legítimo para los fines de perseguir penalmente el cibercrimen y recabar evidencia digital que permita condenar a sus autores; establecer en forma preventiva un sistema de vigilancia o monitoreo online de la población o de personas determinadas.

La Ley Procesal Penal alemana establece una serie de herramientas de investigación orientadas a la prevención de delitos de carácter terrorista, o bien, para permitir la recopilación de evidencia de hechos delictivos cometidos a través de redes telemáticas; entre las que se destacan la inspección del domicilio o las pertenencias de una persona sospechosa, la intervención sus datos y telecomunicaciones, así como su vigilancia personal, domiciliaria, postal o electrónica (Aboso, 2017).

El monitoreo online puede consistir también en la copia remota de los datos almacenados en el disco rígido, controlar el tráfico de correos electrónicos, usar programas intrusivos como troyanos o *keyloggers,* o bien, el encendido remoto de micrófonos o cámaras del sospechoso.

Sin embargo, tal grado de intromisión en la privacidad del imputado, requiere satisfacer un test de razonabilidad y proporcionalidad ante el juez competente que, no en pocos casos, declara la invalidez de un monitoreo online ya que el proceder de los funcionarios trasgrede el derecho de autodeterminación informática del afectado. El bien jurídico protegido que justifica estas medidas, debe tratarse, necesariamente, de uno de primer orden, a saber, la vida, integridad y libertad personal; así como aquellos relacionados al fundamento o existencia del Estado o las condiciones de existencia de las personas.

En lo que respecta a la retención de datos por parte de compañías telefónicas y proveedores de servicios de internet, el Tribunal Constitucional Federal declaró como inconstitucional la legislación que obligaba a dichas compañías a almacenar por el plazo de 6 meses el tráfico de datos con la finalidad de poder ser utilizados en un proceso penal; en la medida que dicho plazo resultaba incompatible con la ley que regula la confidencialidad de las comunicaciones (Velascos, 2016)

En el Derecho norteamericano, por su parte, podemos encontrar como baremo el de la "expectativa de privacidad razonable", generado a partir de la doctrina asentada en el precedente Katz, desde dos perspectivas. Una subjetiva, que se pregunta por el punto de vista del afectado respecto a dicha expectativa; y otra objetiva, que analiza si la sociedad la considera como razonable.

Ambos ejemplos dan cuenta de la necesidad de autorización judicial previa, la proporcionalidad de la medida y la proscripción de fines preventivos, esto es, que existan fundadas sospechas de la participación del imputado en un acto delictivo. Atendido el panorama internacional, difícilmente una iniciativa legislativa que pretenda hacer efectivo lo pretendido por el decreto 866, podría convertirse

en Ley. El hecho que sea posible técnicamente interceptar o espiar nuestras actividades no justifica que esto se realice fuera del control judicial, con fines loables como puede resultar el combate del terrorismo o los ciberdelitos. Sin embargo se mantiene la pregunta de qué podemos hacer frente a estas amenazas.

ACCESO TRANSFRONTERIZO Y COOPERACION INTERNACIONAL.

Si bien el Convenio de Budapest establece nuevos estándares y procura generar términos comunes para que los Estados manejen una legislación similar en materia de ciberdelitos; éste no resulta el primer tratado que regula la cooperación internacional en materia de persecución penal.

Así, por ejemplo, tenemos la Convención de Nassau, ratificada por nuestro Congreso en mayo de 2003, y que dispone la asistencia mutua de los Estados Partes, para investigaciones de delitos merecedores de una pena superior a un año de prisión en el Estado requirente. El tratado dispone actos o medidas a las que un Estado puede negarse si en territorio no es delito el hecho investigado, si la solicitud no es fundada, o bien se advierte que se trata de delitos políticos o tributarios; entre otras excepciones.

La principal innovación del Convenio de Budapest en esta materia, atendida la naturaleza de los delitos; corresponde a lo señalado en su Capítulo III sobre Cooperación Internacional, en lo que dice relación con los procedimientos para requerir asistencia mutua. Se contempla, entre otras medidas, la creación de una Red con puntos de contacto localizables las 24 horas del día, siete días a la semana, con el fin de garantizar una asistencia inmediata para investigaciones sobre delitos informáticos.

Sin embargo, en su artículo 32, el Convenio de Budapest incluye una disposición que autoriza a una Parte la captura de datos sin autorización de otra, esto es, sin los mecanismos de idoneidad, finalidad, proporcionalidad, bilateralidad y visado de la autoridad judicial, en su caso. En particular, la referida norma indica lo siguiente:

> **Artículo 32. Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público.**
> Una Parte podrá, sin autorización de otra:
> a) Tener acceso a datos informáticos almacenados accesibles al público (fuente abierta), independientemente de la ubicación geográfica de los mismos; o

> b) Tener acceso a datos informáticos almacenados en otro Estado, o recibirlos, a través de un sistema informático situado en su territorio, si dicha Parte obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada a revelárselos por medio de ese sistema informático.

Pongamos un caso. La Fiscalía de España, saltándose la autoridad central designada al amparo del Convenio de Budapest, solicita a Movistar Chile datos sobre la conexión de un ciudadano chileno, sin autorización del juez, acogiéndose a lo establecido en el artículo 32 del Convenio de Budapest, respecto del cual Chile no hizo reserva; Movistar Chile entrega la información. Llevémoslo un poco más allá. La Fiscalía de España pide datos a Movistar España sobre la conexión de un ciudadano chileno usuario de un plan de datos de su filial chilena. Movistar España solicita la información a Movistar Chile quien le entrega la información a su Casa Matriz y ésta a la Fiscalía Española.

Otro caso. El Servicio Electoral de Chile (SERVEL) revela los datos del padrón de todos los ciudadanos chilenos mayores de 18 años con indicación de su nombre, número de cédula de identidad y domicilio. Pone a disposición de la ciudadanía un *link* donde dicho padrón puede descargarse, diferenciados por ciudadanos chilenos en territorio nacional y extranjero. Como la página web del SERVEL es una fuente de libre acceso al público, los Estados utilizan la información para notificar a los ciudadanos chilenos extranjeros en su territorio y revisar su situación migratoria.

Finalmente, Amazon o Netflix entregan información sobre datos personales de chilenos usuarios de sus servicios al FBI, sin autorización de juez chileno, pues sus oficinas no se encuentran ubicadas en territorio chileno, por lo que cualquier sanción que el Estado de Chile, en materia de datos personales, podría aplicar es ilusoria.

Estas situaciones, que pueden ocurrir mediante interpretaciones más o menos flexibles de lo que la norma dispone, aprovechando que no se requiere la intervención de otra Parte para legitimar la captura de datos, y encontrándose ratificado el Convenio de Budapest; pareciese que nos traerán los mayores problemas de seguridad nacional -o bien, como se señaló, de soberanía- que las objeciones sobre las modalidades de interceptación en la investigación de delitos informáticos. El Convenio deja una puerta trasera abierta para legitimar la captura de datos personales de fuentes de libre acceso al público; mas sin un recurso que permita a un titular de datos personales solicitar la eliminación de su registro a un Estado del cual no es ciudadano.

El parágrafo 294 del Reporte Explicativo del Convenio de Budapest señala que el artículo 32 regula dos situaciones: cuando los datos que se pretende acceder están libremente a disposición del público, o cuando los datos que se han accedido o recibido por una Parte ubicados fuera de su territorio a través de un sistema informático en su territorio, y que ha obtenido el consentimiento legal y voluntario de la persona que tiene la autoridad legal de revelar los datos a la Parte a través de ese sistema.

En la medida que una persona está legalmente autorizada dependiendo del tipo de persona o de la legislación aplicable, cabe la posibilidad que un organismo persecutor foráneo (en nuestros ejemplos, el FBI o la Fiscalía de España) solicite directamente a un responsable del registro o banco de datos su autorización para acceder a dicha base de datos con el objeto de investigar un delito informático. Esa persona, si bien realiza tratamiento de datos personales de ciudadanos chilenos, perfectamente puede tratarse de una transnacional de origen, por ejemplo, estadounidense, y autorizar a la investigación del FBI en un servidor ubicado en Chile. Incluso puede ser la propia empresa que conserva y trata datos personales de ciudadanos chilenos la que denuncia el hecho a las autoridades de su país de origen.

En consecuencia, este artículo puede dar lugar a accesos remotos a servidores y sistemas de cómputo ubicados en otros países saltándose los canales de asistencia jurídica mutua y otras herramientas de cooperación internacional; que resultan la principal salvaguarda de los derechos de los ciudadanos ya no sólo respecto del actuar persecutor del propio Estado, sino de las agencias de inteligencia u órganos persecutores foráneos.

CONCLUSIONES

Resulta de particular importancia establecer en nuestro país, a la brevedad, una actualización de la obsoleta ley de datos personales (19.628) para evitar la exposición a la que nos encontramos; utilizando como guía el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos. Esperemos que los boletines que se encuentran actualmente en tramitación en nuestro Congreso logren entregarnos, al convertirse en Ley, la protección que necesitamos los usuarios en el ciberespacio, no sólo respecto de estafas o delitos informáticos, sino también del uso indebido que pueden realizar otros Estados respecto de nuestros

datos personales.

Luego de las revelaciones de Wikileaks y Snowden, entre otros, resultan de público conocimiento las acciones de espionaje mutuo que realizan los Estados, a la par del tratamiento masivo de datos de las grandes corporaciones. Sólo una fuerte regulación interna que proteja el oro de nuestra época, permitirá salvaguardar la privacidad y libertades personales de los ciudadanos; manteniendo el control judicial previo como una garantía del Estado frente a las arbitrariedades.

REFERÊNCIAS

Aboso, G. E. (2017). *Derecho Penal Cibernético*. Buenos Aires: Editorial B de F.

Alvarado, A. U. (2014). El control de la resolución motivada que autoriza una interceptación telefónica en Chile y duración de la medida. *Revista de derecho,* 43(1), 421-464. Recuperado el 30 de octubre de https://dx.doi.org/10.4067/S0718-68512014000200011.

Valenzuela, D. A. (2004). Inviolabilidad de las comunicaciones electrónicas. *Revista Chilena de Derecho Informático, 5*(1), paginación indisponible. Recuperado el 30 de octubre de https://dx.doi.org/10.5354/0717-9162.2011.10736.

Velascos, C. (2016). *Jurisdicción y Competencia en relación al Acceso Transfronterizo de Materia de Ciberdelitos*. Valencia: Tirant lo Blanch.