

DERECHOS HUMANOS Y EL DERECHO PENAL EN EL CIBERESPACIO

DIREITOS HUMANOS E DIREITO PENAL NO CIBERESPAÇO

*Pierre Gilles Bélanger**

Resumen: *En la medida en que el tráfico de estupefacientes, el fraude, el blanqueo de dinero y toda una gama de otros delitos trascienden las fronteras nacionales, los responsables de luchar contra esta delincuencia deben encontrar medios eficaces para obtener las pruebas necesarias que, naturalmente, se encontrarán a menudo más allá de sus propias fronteras. Hace ya casi quince años se implementó un instrumento que facilita ese acceso. El Convenio sobre la Ciberdelincuencia, conocido también como Convenio de Budapest sobre la Ciberdelincuencia o Convenio de Budapest, es el primer tratado internacional que intenta abordar los delitos informáticos y los delitos en Internet, incluida la pornografía infantil, armonizando ciertas leyes nacionales, mejorando las técnicas de investigación y aumentando la cooperación entre las naciones y la adecuada protección de los derechos humanos y las libertades en cumplimiento del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. La realidad de 2017 es que la presencia de nuevos elementos, especialmente relativos a la recopilación de datos más personales en el ciberespacio, plantea nuevos desafíos y requiere nuevas ideas. El Convenio permite esta ampliación mediante reflexiones, directrices nuevas y protocolos. Está abierto a todos y es el único instrumento de este tipo. No está completo, sino que deja lugar a la adopción de protocolos futuros y, sobre todo, permite a los grupos de trabajo, entre los regionales que trabajan en el campo de la ciberdelincuencia o la asistencia judicial recíproca, desarrollar nuevas maneras de fortalecer la lucha contra la delincuencia, respetando al mismo tiempo los derechos humanos.*

Resumo: *Na medida em que o tráfico de entorpecentes, fraude, lavagem de dinheiro e uma série de outros crimes transcendem ás fronteiras nacionais, os responsáveis pela luta contra esta delinquência devem encontrar meios eficazes para obter provas necessárias que naturalmente, encontraram-*

* Centro de Derechos Humanos de la Universidad de Ottawa, Canadá.
Las opiniones en este documento reflejan solamente las del autor.
E-mail: Pierre-Gilles.Belanger@justice.gc.ca
Recibido: 21/09/2017. Aceptado: 10/10/2017.

se frequentemente além de suas fronteiras. Há quase quinze anos, foi implementado um instrumento que facilita esse acesso. A Convenção sobre Cibercrime, também conhecida como Convenção de Budapeste sobre Cibercrime ou Convenção de Budapeste, é o primeiro tratado internacional que intenta abordar os crimes informáticos e os crimes em internet, incluindo a pornografia infantil, harmonizando certas leis nacionais, melhorando as técnicas de investigação e acrescentando a cooperação entre as nações e a adequada proteção dos direitos humanos e as liberdades em conformidade com a Convenção Europeia para a Proteção de os Direitos Humanos e ás Liberdades Fundamentais. A realidade de 2017 é a presença de novos elementos, especialmente em relação a coleta de dados mais pessoais no ciberespaço, apresenta novos desafios e requer novas ideias. A Convenção permite essa ampliação através de reflexões, novas diretrizes e protocolos. É aberto a todos e é o único instrumento deste tipo. Não está completo, mas deixa espaço para a adoção de futuros protocolos e, acima de tudo, permite que os grupos de trabalho, entre os regionais que trabalham no âmbito do cibercrime ou assistência judicial recíproca, desenvolvendo novas formas de fortalecer a luta contra crime, respeitando ao mesmo tempo os direitos humanos.

Palabras clave: Convención de Budapest, Cybercriminalidad, Cooperación Jurídica Mutua

Palavras-chave: Convenção de Budapeste, Cibercriminalidade, Cooperação Jurídica Mútua

1. INTRODUCCIÓN

“Los grupos delictivos no han perdido tiempo en abrazar la economía globalizada de hoy y la tecnología sofisticada que la acompaña. Pero nuestros esfuerzos para combatirlos han permanecido hasta ahora muy fragmentados y nuestras armas casi obsoletas. La Convención nos da una nueva herramienta para enfrentarnos al flagelo de la delincuencia como un problema mundial. Con la intensificación de la cooperación internacional, podemos tener un impacto real sobre la capacidad de los delincuentes internacionales para funcionar exitosamente y ello puede ayudar a los ciudadanos de todo el mundo en lo que a menudo es su amarga lucha por la seguridad y la dignidad en sus hogares y en sus comunidades”¹.

El profesor de literatura inglesa y teórico de la comunicación

¹ Kofi Annan, Exsecretario General de las Naciones Unidas. Prefacio a la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus Protocolos. Nueva York: Naciones Unidas, 2004.

canadiense Marshall McLuhan acertó cuando estableció una relación entre el progreso tecnológico y la facilidad extrema con la que pronto podrá recorrerse el globo. Desde luego, la Tierra es la aldea global que previó. Los que trabajamos o hemos trabajado en el ámbito internacional conocemos muy bien que la interconexión sin límites y mundial ha tenido un impacto radical en la asistencia judicial.

El auge tecnológico, el crecimiento de las organizaciones delictivas transnacionales y las respuestas que esto exige a la comunidad internacional crean una situación sin precedentes y plantean continuamente nuevos retos a las instituciones encargadas de luchar contra el crimen que, a su vez, utiliza esta tecnología.

Las investigaciones, los procesos penales, la represión del crimen para proteger a los ciudadanos y el mantenimiento de la paz y del orden público constituyen un objetivo importante en cualquier sociedad organizada. No sería realista que los esfuerzos por alcanzar este objetivo se limitaran a las fronteras nacionales. Así es desde hace mucho tiempo pero es algo cada vez más obvio y urgente en la actualidad y ello plantea nuevos retos².

La asistencia judicial, uno de los mecanismos esencial para combatir la criminalidad, se ha podido desarrollar gracias a la colaboración de los Estados, principalmente en el ámbito de la obtención de pruebas.

En este sentido, se presentan dos desafíos inmensos: la confianza entre los Estados y las herramientas apropiadas en el contexto de la modernidad mencionada.

En la medida en que el narcotráfico, los fraudes, el lavado de dinero y toda una gama de delitos no respetan las fronteras nacionales, los responsables de combatir estos delitos deben encontrar medios eficaces de recoger las pruebas necesarias que, naturalmente, se encontrarán a menudo más allá de sus propias fronteras.

Mi reflexión no tratará sobre la confianza entre los Estados. Como cada cual sabe, se trata de un elemento fundamental que, indudablemente, se forja mediante leyes y buenas prácticas, pero también con muestras de confianza y, a menudo, mediante lazos de amistad. Esto es algo que, muy frecuentemente, se tiende a olvidar o a omitir en el campo de la "asistencia" y que, indudablemente, crea un malestar cuando los funcionarios responsables se marchan con motivo de un cambio de gobierno. Por ello, hay un trabajo enorme por hacer para lograr una estabilidad de la función pública que permita continuar fortaleciendo la asistencia mutua en materia penal y civil. Sin embargo, hablaré más bien de la delicada cuestión de la asistencia en materia penal en el ámbito de un problema más técnico y reciente que requiere reflexiones desde una

² La Corte Suprema de Canadá había identificado bien esta cuestión en los primeros momentos de la Carta Canadiense de Derechos y Libertades. Véase principalmente *États-Unis d'Amérique c. Cotroni R.C.S.* (1989) 48 C.C.C. (3d), p. 193 a 215.

óptica más moderna y que yo calificaría de doblemente internacional: el de la ciberdelincuencia en el contexto de la asistencia judicial.

2. COOPERACIÓN INTERNACIONAL EN MATERIA PENAL EN EL CONTEXTO DE LA CIBERDELINCUENCIA

La cooperación internacional se encuentra en constante progreso, lo cual es en sí mismo una fuente de nuevos retos, tanto para las autoridades que van a recurrir a la cooperación para recopilar pruebas, como para aquéllas a las que corresponde aplicar e interpretar los instrumentos y las disposiciones establecidas por los mecanismos de asistencia.

Mi intención no es sino resaltar los principales desafíos que plantea la ciberdelincuencia, particularmente en el ámbito de la cooperación judicial.

3. CIBERDELINCUENCIA

La ciberdelincuencia es una “industria” multimillonaria cuyas principales víctimas son individuos, instituciones financieras, titulares de propiedad intelectual, gobiernos y muchas otras infraestructuras de carácter estratégico.

Desde mediados de 1990 hasta el 2005 hubo pocas actividades en el ámbito de la ciberdelincuencia. La cuestión fue planteada en los Congresos sobre el Delito de 1990 (La Habana), 2000 (Viena) y 2005 (Bangkok), y como seguimiento al debate de 1990 de la ONU. Un Manual sobre Ciberdelincuencia, producido principalmente con recursos y experiencia canadienses, fue presentado a la Comisión de Prevención del Delito y Justicia Penal, y publicado en 1994.

Un estudio de la ciberdelincuencia por la Secretaría de dicha Comisión fue solicitado por la Comisión de Prevención del Delito y Justicia Penal y el Consejo Económico y Social (ECOSOC) en 1998-1999 y considerado por la Comisión en 2001 y 2002. Fuera de la ONU, las discusiones en la OCDE (1984-86) y el G-7 produjeron el proceso del Consejo de Europa (1997-2000) que eventualmente condujo a la Convención de Budapest en noviembre de 2000. Como resultado, se hizo un llamado expreso a la necesidad de un instrumento internacional.

4. PEQUEÑA HISTORIA DE LA CONVENCIÓN DE BUDAPEST

Es cierto que la Convención de Budapest tiene su origen en el deseo de unir más estrechamente a los miembros del Consejo de Europa pero reconociendo al mismo tiempo el interés por intensificar la cooperación con los otros Estados partes de la Convención. Los

miembros del Consejo estaban convencidos de la necesidad de manera prioritaria una política penal común destinada a proteger a la sociedad del crimen en el ciberespacio, principalmente mediante la adopción de una legislación apropiada y el fortalecimiento de la cooperación internacional. Conscientes de los profundos cambios generados por la digitalización, la convergencia y la globalización de las redes informáticas; preocupados por el riesgo de que las redes informáticas y la información electrónica se utilicen también para cometer delitos penales y de que las pruebas de estos delitos se guarden y transmitan en dichas redes; reconociendo la necesidad de cooperación entre los Estados y la industria privada en la lucha contra la ciberdelincuencia y la necesidad de proteger los intereses legítimos relacionados con el desarrollo de las tecnologías de la información; y considerando que la lucha contra la ciberdelincuencia bien llevada exige una cooperación internacional en materia penal mayor, rápida y eficaz, países de la Unión Europea acordaran de la necesidad de un convenio para prevenir los actos contrarios a la confidencialidad, integridad y disponibilidad de los sistemas informáticos de las redes y de garantizar la penalización de tales conductas mediante la adopción de poderes suficientes para luchar eficazmente contra estos dichos actos ilícitos penales, facilitando la detección, la investigación y el enjuiciamiento, tanto en el ámbito nacional como en el internacional, y previendo disposiciones materiales para una cooperación internacional rápida y fiable.

Éste es el resumen de las razones que mueven a estos países.

La Convención se convirtió, por lo tanto, en el primer tratado internacional sobre los delitos cometidos a través de Internet y de otras sistemas informáticos lidiando particularmente con las infracciones de los derechos de autor, fraude informático, la pornografía infantil, los crímenes de odio, y las violaciones de la seguridad de la red.³ También contiene una serie de poderes y procedimientos tales como la búsqueda en las redes informáticas y la interceptación legal.

Su principal objetivo, enunciado en el preámbulo, es poner en práctica una política penal común encaminada a la protección de la sociedad contra la ciberdelincuencia, especialmente mediante la adopción de una legislación apropiada y el fomento de la cooperación internacional.

Los objetivos de esta Convención consisten principalmente en armonizar los elementos jurídicos sustantivos sobre la delincuencia nacional y las disposiciones conectadas en materia de delito cibernético; en proporcionar poderes jurídicos de procedimientos penales nacionales necesarios para la investigación y enjuiciamiento de tales delitos, así como de otros delitos cometidos por medio de un sistema informático o de evidencia que esté en formato electrónico; y establecer un régimen rápido y eficaz de cooperación internacional.

Los siguientes delitos formen parte del ámbito por la Convención:

el acceso ilegal, la interceptación ilegal de datos, interferencias de datos, interferencia de sistemas, el uso indebido de dispositivos informáticos, falsificación mediante sistemas informáticos, fraude informático, los delitos relacionados con la pornografía infantil, y los delitos relacionados con los derechos de autor y derechos conexos.

También se establecen cuestiones de derecho procesal como la preservación acelerada de los datos almacenados, preservación acelerada y divulgación parcial de datos de tráfico, ordenes de producción, búsqueda y captura de datos informáticos, recolección en tiempo real de datos de tráfico, y la interceptación de datos de contenido. Además, la Convención contiene una disposición sobre un tipo específico de acceso transfronterizo a datos informáticos almacenados que no requiere asistencia mutua (con consentimiento mutuo o cuando esté públicamente disponible) y prevé la creación de una red de 24/7 para garantizar la rápida asistencia entre las Partes Signatarias. Además, como condiciones y garantías, la Convención requiere la provisión de una protección adecuada de los derechos humanos y las libertades fundamentales, incluidos los derechos que se deriven de conformidad con las obligaciones bajo el Convenio Europeo de Derechos Humanos, el Pacto Internacional sobre Derechos Civiles y Políticos y otros instrumentos internacionales de derechos humanos aplicables, y deberá incorporar el principio de proporcionalidad.

Artículo 15: Condiciones y garantías

1. Cada Parte velará por que el establecimiento, implementación y aplicación de las facultades y procedimientos establecidos en esta Sección estén sujetos a las condiciones y garantías establecidas en virtud del derecho nacional, el cual deberá proporcionar la protección adecuada de los derechos humanos y las libertades fundamentales, incluidos los derechos que se deriven de conformidad con las obligaciones que ha asumido en virtud del Convenio del Consejo de Europa de 1950 para la Protección de los Derechos Humanos y las Libertades Fundamentales, el Convenio Internacional de las Naciones Unidas de 1966 sobre Derechos Civiles y Políticos y otros instrumentos internacionales de derechos humanos aplicables, y los cuales incorporarán el principio de proporcionalidad.

La Convención es el producto de cuatro años de trabajo por parte de expertos internacionales y europeos. Ha sido complementada por un Protocolo Adicional que hace de típica la publicación de propaganda racista y xenófoba a través de redes informáticas, similar a lo establecido por las leyes de Difamación Penal. Actualmente, el terrorismo cibernético también se estudia en el marco de la Convención.

5. SU RAZÓN DE SER

La asistencia técnica en materia de ciberdelincuencia ha sido siempre un problema, pero al concluir el proceso europeo, los Estados Miembros no europeos comenzaron a plantear propuestas para lograr un instrumento jurídico universal sobre ciberdelincuencia bajo los auspicios de la ONU. Esto se planteó en el período de sesiones de 2002 de la Comisión, fue el principal tema de debate en el Congreso de Bangkok de 2005, y se volvió a plantear en el proceso preparatorio para el Congreso de 2010 (en El Salvador).

6. NECESIDAD DE TENER UNA “CONVENCIÓN DE BUDAPEST”

Habría que admitir que algunos países hubieran preferido tener tratados regionales cuando se trata del intercambio de información sobre ciberdelincuencia. Desde que entró en vigor, países importantes como Brasil e India se han negado a adoptar la Convención sobre la base de que no participaron en su elaboración³. En general, el trabajo ha contado con la participación de dos grupos opuestos de Estados Miembros, sin que la mayoría de los expertos hayan tomado posición en un sentido o en el otro⁴. Los países del grupo BRIC y afines argumentan que por motivos técnicos y políticos la Convención de Budapest no es una respuesta suficiente al problema y buscan un mandato para la elaboración de un instrumento jurídico universal bajo el auspicio de las Naciones Unidas⁵.

Otros estados como Canadá entre los países no europeos piensan que ésta es la única oportunidad de tener una Convención, alegando que cualquier proceso dirigido a obtener un instrumento jurídico universal podría llegar a un estancamiento permanente o de largo plazo, o resultar en un instrumento muy débil, y apoyan por ello la prestación de asistencia técnica y la promoción de canales informales de cooperación como una respuesta más viable.

7. LA SITUACIÓN ACTUAL DE LA CONVENCIÓN

Hace más de 15 años la Convención de Budapest sobre Ciberdelincuencia surgió para tratar de hacer frente a la ciberdelincuencia mediante la armonización de las legislaciones nacionales, la mejor de las técnicas de investigación, y el aumento de la cooperación entre las

³ Vease <<https://www.cfr.org/blog/coming-soon-another-country-ratify-budapest-convention>>

⁴ Rusia se opone a la Convención, señalando que la aprobación violaría la soberanía rusa, y normalmente se ha negado a cooperar en las investigaciones policiales relacionadas con la ciberdelincuencia.

⁵ Lista de países que han adoptado la Convención: <<http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures>>

naciones. La Convención fue elaborada a finales del decenio de 1990 bajo el auspicio del Consejo de Europa, con la participación activa de un número de estados no pertenecientes al Consejo de Europa, entre ellos Canadá.

La Convención fue adoptada en el año 2001 y entró en vigor en el año 2004. A partir de agosto de 2017, más de 55 estados en la actualidad se han adherido a la Convención, y aunque otros estados han firmado la convención, no la han ratificado todavía.

Naturalmente, se ha desarrollado como la convención internacional para combatir la ciberdelincuencia y promover la Asistencia Jurídica Mutua.

La Convención de Budapest se utiliza como referencia para la redacción de legislación en alrededor 65 Estados adicionales, lo cual la convierte en el instrumento de referencia en más de 130 países alrededor del mundo.

8. DERECHOS HUMANOS EN CANADÁ

Dado el carácter central de las telecomunicaciones en la vida contemporánea, no es extraño que el acceso a la información de suscriptores de Proveedores de servicios de telecomunicaciones (PST) tenga un papel importante en las investigaciones criminales, tanto en Canadá como en el extranjero. La cuestión de acceso a dicha información en Canadá ha sido debatida en una extensa jurisprudencia, incluida la decisión clave de la Corte Suprema de Canadá en esta materia, *R. c. Spencer*, [2014] 2 S.R.C 212⁶. Esta decisión establece que las solicitudes de información relativa a los suscriptores de PSTs (abonados) por parte de las autoridades encargadas de hacer cumplir la ley, pueden implicar una expectativa razonable de privacidad en virtud del artículo 8 de la Carta canadiense de derechos humanos. Este es un grado de expectativa de privacidad que normalmente requiere que las agencias policiales obtengan autorización judicial para adquirir la información de conformidad con las normas constitucionales canadienses. El problema radica en el tiempo que pueda tomar la ostensión de la autorización judicial. La mayoría de nuestros países enfrenta los mismos problemas en materia de derechos humanos que surgen a dentro de las acciones de cooperación internacional en un mundo en el que la información requerida no solamente extremadamente sensible sino también volátil. Asimismo la decisión en el caso *Spencer* en Canadá, resalta las expectativas de privacidad que puedan surgir no sólo de la información propia del suscriptor, sino también de aquella que pueda revelarse a través de la vinculación de esta información con

⁶ El artículo 8 de la Carta canadiense de derecho humano dispone lo siguiente: “Toda persona tiene derecho a estar protegida de una búsqueda del estado no razonable” y ha sido interpretado por el Tribunal Supremo de Canadá como una protección a la interferencia estatal irrazonable con la expectativa razonable de privacidad de un individuo.

otra información. Estas son los retos que presenta el almacenamiento e intercambio de información en la “nube”. ¿Cómo podemos garantizar los derechos humanos incluyendo el derecho a la privacidad, y al mismo tiempo combatir de manera efectiva la cibercriminalidad en esta nueva realidad cibernética donde la información viaja a la velocidad de la luz? Obviamente, estas situaciones nos llaman a nuevas realidades.

9. LA NUEVA REALIDAD

La Convención sigue siendo oportuna y pertinente en la actualidad, reflejando sus objetivos generales y su dinámica de crecimiento. Dicho esto, resultaba imposible que sus negociadores, hace 20 años, pudieran prever el aumento exponencial del uso de los dispositivos electrónicos, de sus usuarios, así como de las correspondientes pruebas digitales que se recabarían en las investigaciones penales como resultado de esta tendencia.

En el mundo actual de la omnipresente comunicación móvil, los teléfonos celulares y las tabletas nos acompañan a todos lados; las computadoras se localizan tanto en los hogares como en nuestros vehículos. Estos dispositivos electrónicos son, de igual forma, una parte indispensable en la vida cotidiana de quienes llevan a cabo actividades delictivas.

Por lo tanto, el volumen de la prueba digital continua creciendo tanto en los casos de delitos cibernéticos como en aquéllos más “tradicionales”, ya que los delincuentes se apoyan en el uso de aparatos electrónicos a la hora de planificar y llevar a cabo secuestros, tráfico de drogas, ataques terroristas, etc. Los investigadores y los fiscales requieren un constante acceso a la prueba digital para investigar estos delitos y proteger al público. Sin embargo, algunos de estos datos son almacenados en el extranjero o en “la nube” por proveedores multinacionales de servicios, lo cual complica considerablemente la recopilación de la prueba digital.

La Convención de Budapest ya contiene mecanismos para, entre otras cosas, preservar información digital almacenada en el extranjero y brindar acceso a dicha información a través de Tratados de Asistencia Jurídica Mutua (MLAT, por sus siglas en inglés).

Sin embargo, este sistema es oneroso y se ve cada vez más abrumado por el volumen de solicitudes de asistencia (el promedio del tiempo de respuesta a estas solicitudes varía entre 6 y 24 meses).

10. NUEVAS NECESIDADES EN ASISTENCIA JURÍDICA MUTUA

Las exigencias de la realidad actual, crean la necesidad de cooperar con los encargados de hacer cumplir la ley, en la obtención de evidencia en servidores situados en “jurisdicciones extranjeras, múltiples o desconocidas”. Se debe ahondar más, sobre las soluciones para acceder a dicha evidencia -

existente en la nube - relativa a los fines de la justicia penal.

La convención permite nuevos protocolos y, en uno de ellos, se puede encontrar herramientas que permiten una asistencia jurídica mutua más eficaz; a fin de facilitar la cooperación directa con los proveedores de servicios para enmarcar y establecer condiciones y garantías; concernientes a las prácticas existentes de acceso Transfronterizo a los datos y establecer los requisitos de protección de los mismos.

A la luz de la proliferación de la ciberdelincuencia y otros delitos relacionados con evidencia electrónica, y en el contexto del cambio tecnológico y la incertidumbre respecto a la jurisdicción, son necesarias soluciones adicionales que permitan a las autoridades de la justicia penal obtener “evidencia electrónica específica en materia de investigaciones penales concretas” en un marco respetuoso de derechos humanos.

Todos estarán de acuerdo en que se necesita un régimen simplificado, para las solicitudes de asistencia jurídica mutua para obtener información sobre el suscriptor. Se debe pensar entonces en - quizás - aceptar órdenes internacionales de presentación de información; se debería pues tener cooperación directa entre las autoridades judiciales en las solicitudes de asistencia jurídica mutua; realizar investigaciones conjuntas y formar equipos internacionales de investigación. Para facilitar la comunicación se podrían limitar, a dos o tres, los idiomas más hablados para recibir solicitudes; y poder realizar audiencias mediante audio y vídeo de testigos, víctimas y expertos; y un nivel de procedimientos de emergencia para la Asistencia Jurídica Mutua, etc.

Tener disposiciones que permitan la cooperación directa con los proveedores de servicios en otras jurisdicciones con respecto a las solicitudes de información del suscriptor, sería lo más conveniente, para la preservación de la información y la gestión de las solicitudes de emergencia. La ausencia de un marco más claro y una mayor protección de las prácticas existentes de acceso transfronterizo a los datos, incluyendo las salvaguardias y los requisitos de protección de datos, dificulta los procesos.

Si bien no es necesario estar de acuerdo con todas esas posibles adiciones o elementos, es evidente que los Grupos de Trabajo y las autoridades centrales de todo el mundo deben pensar acerca de esta nueva realidad que pide mejorar las prácticas actuales en el contexto de la ciberdelincuencia.

Este es el motivo por el cual, como un elemento mínimo, la Convención deberá ser ratificada por los países y se debe seguir trabajando sobre ello en un proceso de negociación en la mesa internacional tal como la Convención de Budapest lo permite para todos los países.

La Convención de Budapest es la única herramienta eficaz para la

cooperación y el cumplimiento de la ley en materia de ciberdelincuencia, así como es su garantía para la libertad de expresión y los derechos humanos, y que también permite nuevas formas y protocolos adicionales que - eventualmente - podrían ser la razón de ser del grupo de trabajo regional, como el de la OEA.

CONCLUSIÓN

La Convención de Budapest es el único intento ampliamente reconocido para tratar cuestiones de ciberdelincuencia y contiene la tipología más aceptada para la ciberdelincuencia. En marzo de 2015, Canadá aprobó una legislación llamada “la Ley sobre la Protección de los Canadienses contra la Ciberdelincuencia” y entró en vigor, lo cual incluyó cambios legislativos que permitieron a Canadá ratificar la Convención, el 8 de julio de 2015.

Por lo tanto, el país se ha comprometido a aumentar el número de partes en la Convención de Budapest, en lugar de embarcarse en el incierto proceso de negociar por separado cualquier nuevo instrumento. Es como un efecto dominó. Una vez que un país se une al grupo, sabe que una cooperación mutua es necesaria, beneficiosa y esencial. En cierto modo somos afortunados de que más y más países crean en la Convención, ya que es la única manera de tener una adecuada cooperación - Volvemos a hablar de confianza y yo prometí al comienzo que no hablaría de ello.

Habrán muchos nuevos problemas emergentes en materia de cooperación internacional, obre la ciberdelincuencia y cómo se trata (o puede ser tratada) mediante la aplicación del citado instrumento internacional. Los datos albergados en las nubes, plantean una serie de desafíos a la justicia penal, en particular con respecto a la legislación aplicable y la jurisdicción para hacer cumplir la ley. Dadas las múltiples configuraciones para el lugar dónde están situados los proveedores de servicios, dónde se almacenan los datos, etc., es cada vez más difícil para las autoridades determinar qué régimen jurídico se aplica a los datos.

Los grupos de trabajo deben seguir explorando soluciones sobre el acceso de la justicia penal a la evidencia almacenada en servidores en la nube y en jurisdicciones extranjeras, incluso mediante la asistencia jurídica mutua. Llevando a cabo las buenas prácticas y la Nota de Guía para tratar la cuestión de las órdenes de presentación nacionales, para la obtención de la información del suscriptor en virtud del Artículo 18⁷ de

7 Artículo 18 - Orden de Presentación

1. Cada Parte deberá adoptar las medidas legislativas y de otra índole que sean necesarias para facultar a sus autoridades competentes a ordenar:

a) a una persona en su territorio que presente datos computacionales específicos que estén en posesión o bajo control de esa persona, que estén almacenados en un sistema computacional o un medio de almacenamiento de datos de computadora; y

la Convención de Budapest, es un buen ejemplo. Aunque las Notas de Guía no crean nuevas obligaciones jurídicas, se puede esperar que sean fuentes influyentes de interpretación de las disposiciones del tratado.

Obviamente, esto plantea algunos problemas potenciales. Por ejemplo, el artículo 18.1.b de la Convención debe entenderse en el sentido de que, las autoridades competentes de una Parte deben ser capaces de solicitar información del suscriptor de parte de un proveedor de servicios, que ofrezca un servicio en su territorio, independientemente de dónde se almacena la información. Esto plantea preguntas tales como: si ello pretende o no extender la jurisdicción para órdenes de presentación “nacionales” más allá de los parámetros aceptados de territorio y nacionalidad, en la medida en que pudieran considerarse “extraterritoriales”.

Hay una serie de temas más amplios que deben considerarse. Nota al artículo 18.1.b, incluyendo su impacto en cuestiones de soberanía, en los esfuerzos para ampliar la cobertura de la Convención y en el debate en curso sobre si un nuevo tratado mundial, sobre la ciberdelincuencia, es necesario. Por otro lado, queda claro que alguna solución tendrá que encontrarse para facilitar las investigaciones de delitos cibernéticos. La cuestión del acceso transfronterizo a la información del suscriptor, ya está siendo probada en los tribunales y en la realidad, ya que la práctica de emitir las órdenes de presentación de información sobre el suscriptor directamente a los proveedores de servicios ubicados en otras jurisdicciones, parece estar sucediendo ya (con las respuestas de los proveedores de servicios ofrecidas sobre una base voluntaria).

Otro punto de preocupación es que, aunque algunos países, como Rusia y China están buscando activamente un mayor control sobre el contenido y el uso de Internet, está claro, desde nuestro punto de vista, que es demasiado tarde para volver hacia atrás hacia un sólo instrumento regional o un instrumento más amplio. Ya fuimos muy lejos y un protocolo adicional, para resolver algunos ajustes es el único camino que debemos seguir. Pero seamos justos, y digamos que este debate está manifestándose en un número creciente en varios foros internacionales - con la ciberdelincuencia siendo uno de los aspectos del debate más amplio sobre la gobernanza de Internet. Hay presión proveniente de ciertos países para crear un nuevo tratado de la ONU sobre la ciberdelincuencia. Si esto será posible algún día no lo sabemos, pero no perdamos de vista la importante herramienta que tenemos ahora y tratemos de mantener las discusiones centradas en los resultados más prácticos y alcanzables, en la materia. La realidad es que esperar por un tratado de la ONU, con el fin de fortalecer las asociaciones

b) a un proveedor de servicios que ofrece sus servicios en el territorio de la Parte que presente la información del suscriptor relativa a dichos servicios que esté en posesión o control del proveedor de servicio.

para la asistencia técnica y la creación de capacidad para combatir la ciberdelincuencia con Estados Miembros o las organizaciones pertinentes, el sector privado y la sociedad civil; o esperarlo antes de proveer la asistencia técnica, podría ser contraproducente para la lucha contra la ciberdelincuencia. Existe la necesidad de centrar la atención para completar Estudios Integrales sobre este tipo específico de delincuencia, en el interior de lo que tenemos ahora y responder a las urgentes necesidades de la nueva tecnología.

Al final, es cierto que necesitamos este pedazo de legislación internacional más que para ayudar, para darnos parámetros de trabajo entre nosotros. Como decía uno de mis antiguos colegas de Paraguay, “una aplicación eficaz no se limita a la legislación y a la administración”. La cosa va mucho más lejos. Un país puede disponer de un excelente programa legislativo y convencional de asistencia y procedimientos administrativos bien establecidos y, a pesar de ello, verse en la imposibilidad de ofrecer una ayuda eficaz porque el mejor sistema no vale, lo que valen las personas que lo utilizan en la práctica. A menudo, el éxito de la asistencia depende casi totalmente del conocimiento y, lo que es aún más importante, de la flexibilidad de las autoridades que solicitan y, sobre todo, que prestan la ayuda.

RESUMEN BIOGRÁFICO

Pierre Gilles Bélanger es Abogado canadiense. Hoy está realizando un doctorado en derecho que examina el tema de la reforma penal que está teniendo lugar en toda América Latina y el análisis para proponer una nueva forma sostenible de desarrollo legal. Bélanger desde 2012 ha sido responsable de un proyecto de investigación sobre América Latina y los derechos humanos en el Centro de Derechos Humanos de la Universidad de Ottawa. Él fue de 2000 a 2007 coordinador de un nuevo grupo de trabajo ante la OEA en cooperación jurídica en materia penal. En 2010 y 2014, impartió clases en la facultad de relaciones internacionales y derecho en México como profesor visitante en el Tecnológico de Monterrey. Obtuvo en 2011 la certificación del Tecnológico de Monterrey sobre la reforma penal en México. Desde 2012, ha establecido un programa de pregrado entre la Universidad de Ottawa y varias universidades de América Latina, titulado “El orden jurídico y político en América Latina y sus relaciones con Canadá”. Actualmente está coordinando para la Facultad de Derecho Común un proyecto de capacitación en derechos humanos para jueces en México y consejo jurídico al Ministerio de la Justicia de Canadá.