La Convención de Cibercrimen de Budapest y América Latina

Breve guía acerca de su impacto en los derechos y garantías de las personas

Volumen 1

por los Derechos Civiles

Área Digital
Asociación por los Derechos Civiles

Marzo 2018
https://adcdigital.org.ar

Este trabajo fue realizado como parte de un proyecto financiado por Ford Foundation.

Índice

La Convención de Cibercrimen de Budapest y América Latina: Breve guía acerca de su impacto en los derechos y garantías de las personas*

I. Las garantías del proceso penal

La aplicación de una pena sobre un individuo constituye una de las muestras más acabadas de la intensidad que puede asumir el castigo estatal. Esta afirmación se vuelve clara con solo pensar en el modo más usual en que una persona encontrada culpable de un delito es afectada: a través de la pérdida de su libertad. Con la pena de muerte eliminada -legalmente o de facto- en la mayoría de los países latinoamericanos[1] y sin dejar de tomar en cuenta la existencia de otras penas que impactan ya sea en el patrimonio (en el caso de la pena de multa) o en la capacidad para ejercer algún cargo, profesión o función (el caso de la pena de inhabilitación), la detención o arresto de una persona para ser encerrada en una prisión se transforma así en el ejemplo paradigmático de sanción penal.

La gravedad de este castigo ha llevado a que su aplicación esté prevista únicamente para aquellas situaciones en donde se haya demostrado que no puede utilizarse una forma menos grave de sanción. En términos jurídicos, a esta directiva se la conoce como el principio de subsidiariedad o "ultima ratio penal" y es un reflejo de la idea de que una sanción de tal envergadura no puede ser aplicada ante cualquier mala conducta, por más reprochable que sea. Es por eso que la tarea de creación de delitos debe ser llevada a cabo con sumo cuidado, a fin de evitar que una utilización excesiva del derecho penal sirva como excusa para la expansión de prácticas represivas por parte del Estado.

*El presente documento fue escrito por **Eduardo Ferreyra**, analista de políticas públicas del Área Digital de la Asociación por los Derechos Civiles (ADC). Encargado de diseño y diagramación: Leandro Ucciferri.

[1] En la actualidad Cuba y Guatemala son los únicos países latinoamericanos que contemplan en su legislación la posibilidad de aplicación de la pena de muerte. A su vez, Brasil, Chile, El Salvador y Perú la mantiene para delitos excepcionales cometidos en tiempos de guerra. En el resto de los países, la pena de muerte se encuentra abolida legalmente o de hecho. Ver Informe Global de Amnistía Internacional. Condenas a muerte y ejecuciones (2016), disponible en https://www.amnesty.org/download/Documents/ACT5057402017SPA (último acceso: 29/01/17).

Pero establecer límites a las conductas sujetas a sanción penal es solo un primer paso. Si el Estado castiga por un delito a quien no lo cometió o si efectivamente castiga a quien lo hizo pero a costa de haber violado su dignidad, intimidad, integridad, etc., el resultado seguirá siendo insatisfactorio e injusto. Es por ello que a la par de determinar las conductas que serán merecedoras de pena, también se deben establecer una serie de pasos que los poderes públicos deben seguir para poder aplicar una pena a la persona acusada de un delito determinado. Esto es lo que se conoce como "proceso penal". Y al igual que en el caso de la creación de delitos, los criterios a seguir al momento de diseñar un proceso penal deben respetar ciertos principios considerados fundamentales para una sociedad democrática. Uno de los más importantes es el respeto a los derechos del acusado.

Si pensamos en la desigualdad de condiciones -en términos de recursos, poder, y capacidades- que se presenta en la relación entre el Estado y el individuo sometido a una investigación, resulta lógico que ese desbalance debe ser compensado por la creación de ciertos requisitos que el poder público debe cumplir para poder condenar a una persona. Esta protección se encuentra consagrada a través de las llamadas "garantías del proceso penal". La función de estas garantías es limitar el accionar estatal, a fin de que sus amplias facultades sean ejercidas de un modo que respete la dignidad de las personas.

Las garantías son diversas y entre las más importantes se cuentan las siguientes[2]:

La presunción de inocencia: reflejada en la famosa frase "toda persona es inocente hasta que se demuestre lo contrario", significa que el acusado no debe probar que es inocente, sino que es el poder público el que debe reunir la prueba necesaria para condenarlo. Además, el acusado debe ser considerado inocente hasta el momento en que sobre él recaiga una condena firme, es decir, sin posibilidad de ser apelada ante otro juez o tribunal. Este principio es el que suele ser tenido en cuenta al momento de considerar como excepcionales medidas la prisión preventiva, en el que una persona es encarcelada sin que haya una sentencia que la haya declarado culpable.

En caso de duda, se interpreta a favor del acusado: más conocido por la expresión latina "in dubio pro reo", esta garantía establece que la única forma de condenar a una persona es demostrando de manera *indudable* su participación en el delito del cual se lo acusa. Por lo tanto, si no hay certeza sobre las circunstancias en que se produjo el delito, sobre la autoría o sobre el estado mental del acusado, este no debería ser condenado.

Duración razonable del proceso: la persona no puede estar sujeta a un proceso judicial que se extienda indefinidamente en el tiempo, más en un proceso penal, en el cual su libertad puede

[2] Para ampliar el estudio sobre el vínculo entre derechos humanos y garantías penales puede consultarse Cafferata Nores, José Ignacio. Proceso penal y derechos humanos : la influencia de la normativa supranacional sobre derechos humanos de nivel constitucional en el proceso penal argentino. 2a ed. 1a reimp. - Ciudad Autónoma de Buenos Aires : Del Puerto, 2011. Disponible en https://www.cels.org.ar/web/wp-content/uploads/2016/10/Proceso-penal-y-derechos-humanos.pdf (último acceso: 29/01/18).

estar en juego. Esta situación se agrava si el acusado se encuentra en prisión preventiva. Es por eso que el Estado debe realizar los procesos en un lapso de tiempo razonable, de acuerdo a la complejidad del delito y de la investigación, pero sin que esto sirva como excusa para someter al acusado a una situación de incertidumbre judicial que dure muchos años.

Imparcialidad judicial: el acusado debe tener la certeza de que la decisión sobre su culpabilidad o inocencia será tomada por un juez o tribunal exclusivamente en base al análisis de las pruebas aportadas durante el juicio. Asimismo, no debe haber ninguna sospecha de que por algún motivo, el juez tenga preferencia por alguna de las partes del juicio. Este principio tiene una especial aplicación en la separación de las funciones de investigar-acusar y la de juzgar. A fin de respetar el principio de imparcialidad, resulta conveniente que la primera función esté en manos de un órgano (Fiscalía, Ministerio público) distinto al órgano que va a juzgar y eventualmente sentenciar (jueces). Así, tanto el acusado como los acusadores están en pie de igualdad frente a un tercero (juez) encargado de decidir el conflicto. Este sistema es conocido como "acusatorio" y se distingue del sistema "inquisitivo" en el cual el juez investiga, acusa y juzga. En la actualidad, existe una tendencia en los sistemas jurídicos de pasar de un modelo "inquisitivo" a uno "acusatorio" a fin de adecuarse más al principio de imparcialidad[3].

II. La intimidad y las nuevas técnicas de investigación penal

Un aspecto importante de la protección de las garantías del individuo es su intimidad. Como se dijo anteriormente, para poder condenar a una persona es necesario recolectar prueba que demuestre de manera notoria su participación en el delito del cual se la acusa. Muchas veces -si no todas- esas pruebas se encuentran en ámbitos propios de la persona, como su domicilio. Así, las medidas que se lleven a cabo para obtener aquellas pruebas deben tener el cuidado de no afectar el derecho a las personas a su intimidad. Es por eso que -en este caso- las garantías tienen como objetivo proteger a la persona de posibles abusos e intromisiones arbitrarias en su espacio personal. Entre las principales restricciones figuran: la creación de una ley en donde se establecen las causales por las cuales se puede entrar en el domicilio de la persona, el dictado de una orden de allanamiento dictada por un juez de manera previa y que las razones para entrar al domicilio sean respetuosas de una sociedad democrática[4].

Ahora bien, las garantías procesales que protegen la intimidad fueron diseñadas para regular las investigaciones que se llevan a cabo sobre entornos físicos. Sin embargo, en la actualidad un número

[3] A diferente ritmo y con sus propias variantes internas, la mayoría de los países latinoamericanos -Argentina, Chile Colombia, entre ellos-, han ido adoptando modelos acusatorios desde principios de este siglo.. Otros como México y Uruguay se encuentran en procesos de transición al mismo, mientras que existen excepciones como Brasil, que es el único país latinoamericano que todavía mantiene un sistema penal inquisitivo.

[4] Ibid. pág. 101-105.

cada vez mayor de casos son investigados o resueltos en base a la utilización de evidencia digital. La popularización de dispositivos tecnológicos ha posibilitado la aparición de nuevas conductas delictivas (los llamados delitos informáticos, como por ejemplo, el acceso no autorizado a un sistema informático) o han permitido que se cometan delitos tradicionales (estafas, fraudes, etc.) a través de medios tecnológicos. Así, las investigaciones han tenido que recurrir a métodos de recolección de prueba que sean adecuados a la característica digital de la misma y que por ende son distintos a los utilizados tradicionalmente[5].

Este cambio en la forma en que se efectúan las investigaciones ha hecho surgir el interrogante de si las reglas existentes son adecuadas para proteger la intimidad de las personas acusadas. Pensemos por ejemplo en un allanamiento. Uno de los requisitos principales es que la orden judicial debe establecer el lugar a ser allanado y la prueba que se quiere obtener. De esta manera, la actividad de la policía se encuentra limitada a buscar únicamente lo que se ordena y en los lugares en los que razonablemente pueda estar, evitando así acceder a lugares sobre los cuales no hay justificación para hacerlo. Si lo que se busca es un revólver, la policía no está autorizada a revisar libros o cuadernos.

En el caso de la prueba digital, ya sea que se secuestre la computadora o se realice el procedimiento en el mismo sitio allanado, la cuestión se vuelve más engorrosa. Esto es así debido a que la evidencia que se busca no es la computadora sino los archivos que están dentro de ella. Pero como cualquiera sabe, en una computadora existen miles de archivos, los cuales pueden estar a completa disponibilidad de los investigadores, aunque no tengan ninguna relación con el delito que se está investigando. Por lo tanto, ordenar el secuestro o registro de una computadora puede resultar excesivo y contrario al requisito de que el allanamiento sea particular y específico, al menos si lo pensamos con las reglas tradicionales.

Por otro lado, la información que se necesita puede no estar en la computadora del acusado sino alojada en servidores externos de las empresas que ofrecen los servicios utilizados por aquél. Pensemos en los correos electrónicos, los archivos guardados en la "nube" o las claves de acceso a cuentas. En estos casos, las fuerzas de seguridad pueden solicitar directamente a la empresa la entrega de dicha información, procedimiento del cual el acusado puede no estar ni enterado.

Finalmente, las pericias oficiales en casos penales son llevadas a cabo en general por miembros de alguna fuerza oficial (policial, judicial, o de característica similar), que suelen tener departamentos encargados de la realización de este tipo de trabajos. Esto es una diferencia respecto a un proceso civil, en el cual los peritos oficiales son elegidos de un listado de peritos que posee el Poder Judicial. Esta situación supone el riesgo de colocar al acusado en una posición de desigualdad de conocimiento frente a las fuerzas encargadas de la investigación. Esto es así, ya que el entendimiento sobre las

[5] Para profundizar sobre el impacto de las tecnologías digitales sobre el proceso penal, ver Kerr, Orin S., Digital Evidence and the New Criminal Procedure. 105 Columbia Law Review 279 (2005); GWU Law School Public Law Research Paper No. 108. Disponible en SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=594101 (último acceso: 29/01/2018)

formas digitales de recolección de evidencia requieren un conocimiento específico sobre Informática que la mayoría de las personas no posee. De esta manera, la posibilidad de controlar la legalidad del procedimiento presenta más obstáculos que en el caso de un allanamiento normal en donde el acusado puede estar presente observando la actividad policial.

III. La Convención de Budapest como iniciativa internacional

Estas diferencias -y otras más que no han sido mencionadas- han sido causa de que las autoridades hayan empezado a pensar en la elaboración de regulación específica[6] que aborde la cuestión de la prueba digital. Junto con esto, había otra razón importante: en estos casos, la investigación y recolección de evidencia requiere muchas veces la cooperación internacional. Los delitos que se cometen en y a través de la red suelen tener carácter transnacional, ya sea porque son cometidos por personas que operan en diferentes países, porque las víctimas están en un país distinto o porque la prueba está alojada en servidores ubicados en países distintos al que lleva adelante la investigación. Es por ello que las investigaciones suelen requerir la intervención de diferentes Estados. A su vez, esto dio impulso a que hayan surgido iniciativas de regulación por parte de organismos internacionales.

En este sentido, la iniciativa más importante fue adoptada en noviembre del 2001, cuando el Consejo de Europa[7] sancionó el Convenio sobre Cibercrimen, más conocido como "Convenio de Budapest"[8] debido a la ciudad en donde fue adoptado. El convenio entró en vigor en 2004 y constituye hasta el momento el único instrumento internacional que aborda de manera específica el tema de cibercrimen. Si bien el tratado fue creado en el seno de una institución europea, está abierto para que otros estados puedan adherirse. Actualmente, hay 56 estados parte que provienen de los cinco continentes. Por el lado de América Latina, ya son parte Chile, Costa Rica, República Dominicana y Panamá. Seguramente, Argentina se unirá muy pronto, debido a que la adhesión al Convenio fue aprobada por el Congreso y sólo resta depositar el instrumento de adhesión[9]. Asimismo, México, Colombia,

[6] Frente a la ausencia de normativa específica se han desarrollado protocolos o reglas de buenas prácticas. Entre las más importantes a nivel internacional se encuentran la ISO/IEC 27037:2012 Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence y la ISO/IEC 27042:2015 Information technology -- Security Techniques -- Guidelines for the Analysis and Interpretation of Digital Evidence. A pesar de que no son obligatorias suelen ser seguidas por diversas fuerzas encargadas de recolectar prueba digital. El tema de la práctica forense será abordado en otro documento.

[7] El Consejo de Europa es una organización internacional creada en 1949 con el fin de promover la cooperación entre los países de Europa y afianzar los valores de la democracia, los derechos humanos y el estado de derecho. En la actualidad abarca a casi todos los países del continente europeo y no debe ser confundido con otros organismos más conocidos como la Unión Europea.

[8] Convención sobre cibercrimen, disponible (en inglés) en https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (último acceso: 29/01/18). Existe una traducción no oficial al español disponible en https://rm.coe.int/16802fa41c (último acceso: 29/01/18)

[9] Cibercrimen. La Argentina adhirió al Convenio de Budapest. Ministerio de Justicia, disponible en http://www.vocesporlajusticia.gob.ar/argentina-adhirio-al-convenio-de-budapest/ (último acceso: 29/01/18)

Paraguay y Perú están en proceso de ratificar el Convenio. Por su parte, Brasil es reticente a formar parte de este instrumento bajo el argumento de que no participó en su creación y de que el ámbito más adecuado para la adopción de un convenio de este tipo es Naciones Unidas[10].

El Convenio de Budapest consta de 48 artículos divididos en cuatro capítulos, con sus respectivas secciones. El primer capítulo se encarga de definir términos como "sistema informático", "dato informático", "proveedor de servicio" y "datos de tráfico".

El segundo capítulo se encarga de establecer las medidas que deben ser tomadas a nivel nacional por los estados parte. En este apartado, el convenio establece la necesidad de criminalizar determinadas conductas que se realizan mediante dispositivos tecnológicos. Entre ellas están: el acceso ilícito a un sistema informático, la interceptación ilícita de datos, el abuso de dispositivos, el fraude informático y delitos relacionados con pornografía infantil y propiedad intelectual. Asimismo, también se establecen medidas sobre la forma en que debe llevarse a cabo el procedimiento de investigación. Así, encontramos disposiciones sobre conservación rápida de datos (para evitar que sean eliminados antes que se inicie o finalice la investigación), registro y secuestro de dispositivos, obtención en tiempo real de datos de tráfico o interceptación de contenido.

El tercer capítulo trata sobre cooperación internacional y establece disposiciones sobre asistencia mutua en temas como extradición o acceso, conservación, obtención en tiempo real e interceptación de datos. Finalmente, el capítulo final se refiere a cuestiones de entrada en vigor, forma de adhesión de los estados y las reservas que pueden hacerse al momento de incorporarse.

IV. Pros y contras de la adopción de la Convención en América Latina

La conveniencia de adherirse a este instrumento suele ser justificada en la ausencia de reglas que se refieran de manera específica a la prueba digital y en la necesidad de alcanzar acuerdos internacionales para facilitar la cooperación en la investigación de delitos. Si bien estos motivos son legítimos, también existen otras cuestiones que deben ser analizadas con cuidado. A continuación enumeramos algunas de ellas:

- Al ser un documento emanado del Consejo de Europa, solamente aquellos integrantes del mismo pudieron participar en su redacción. De esta manera, los demás países -entre ellos, los países latinoamericanos- no tuvieron ninguna oportunidad de tomar parte en la discusión y dar su opinión en los debates previos a su adopción. Así, cuestiones sensibles para la política y la soberanía de un país -como la adecuación de la legislación penal o procesal penal, el establecimiento de los términos de la cooperación internacional o la legitimidad de accesos de

[10] Cfr. Non-paper presentado por Brasil ante la Comisión sobre Prevención del Delito y Justicia Criminal de Naciones Unidas (2015), disponible en inglés en United Nations Office on Drugs and Crime (último acceso: 29/01/17)

otros países a sistemas alojados en el propio- serán influidos por un Convenio en cuya redacción no hubo intervención de nuestros países. Esto debería ser motivo para exigir mucha atención en el análisis de las disposiciones, a fin de comprobar si éstas son o no capaces de servir a nuestros objetivos políticos o a nuestros principios.

- El art. 4 del Convenio establece que debe considerarse como un delito la alteración, daño o supresión de datos informáticos cuando es hecha de manera ilegítima. Sin embargo, no establece ningún requisito acerca de la magnitud o importancia que debe tener el daño para poder ser criminalizado. Así, se perjudica el principio de que el derecho penal, en una sociedad democrática, debe ser concebido como un derecho al cual se debe recurrir como último recurso y en casos excepcionales. Si bien el artículo sí establece que los estados pueden reservarse el derecho a penalizar únicamente aquellos actos que comporten "daños graves", basta que un Estado no hago uso de dicha reserva para que quede legitimado a criminalizar toda conducta, sea grave o no. Este es el caso de Argentina, en donde ya existía este delito con anterioridad[11] y en donde no se estableció el requisito de la gravedad[12].

- El art. 6 determina que se debe penalizar el abuso de dispositivos -incluidos programas informáticos- que puedan utilizarse para cometer delitos informáticos. La ambigüedad de la redacción podría llevar a criminalizar una práctica habitual en la comunidad técnica, como es el diseño y utilización de software para la investigación de problemas de seguridad, el cual también puede ser utilizado para cometer delitos. La ausencia de una mayor especificación podría traer el peligro de que investigadores y expertos en seguridad informática puedan sentirse inhibidos de hacer su trabajo y alertar sobre potenciales fallas de seguridad que afectarían a los ciudadanos.

- El art. 10 establece la obligación de considerar como delitos las infracciones sobre derechos de propiedad intelectual que se realicen a gran escala y por medio de un sistema informático. Esta disposición constituye un preocupante impulso para los reiterados intentos de criminalizar el intercambio de información que tiene lugar en Internet, los cuales no tienen en cuenta otros derechos en juego, como la libertad de expresión y el derecho al acceso al conocimiento. En un contexto como el argentino, en donde actualmente se está discutiendo la necesidad de reformar la ley de propiedad intelectual, esta disposición puede servir como justificativo para promover una legislación más represiva, sin preguntarse por la efectividad de la misma para resolver los problemas que pretende solucionar.

[11] La ley 26.388 de reforma del Código Penal fue sancionada en 2008 e incorpora diversos delitos informáticos. Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm (último acceso: 29/01/18)

[12] El actual art. 183 del Código Penal establece en su segundo párrafo que "en la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos..."

- En materia investigativa, la Convención otorga amplios poderes a los estados para que lleven adelante actividades de vigilancia y de acceso a datos personales. Entre las acciones autorizadas, se encuentran: ordenar la conservación rápida de datos informáticos (procedimiento conocido como "quick freeze") e incluso su revelación rápida cuando se trate de datos de tráfico[13], el registro y secuestro de dispositivos informáticos, el acceso a sistemas informáticos, la obtención de datos en tiempo real y la interceptación de contenido de las comunicaciones. Como se ve, todas estas acciones tienen el potencial de afectar gravemente la privacidad de las personas, ya que implica que una gran cantidad de información personal estará a disposición de las autoridades y las fuerzas de seguridad.

- A pesar de la sensibilidad de las facultades señaladas anteriormente, la Convención no establece de manera detallada las condiciones y salvaguardas que deberían tomarse para evitar que dichos poderes sean usados de manera perjudicial para las personas. La norma deja la determinación de aquellas garantías a la legislación interna de cada país y sólo hace referencias genéricas a que los países deben *"garantizar una protección adecuada de los derechos humanos y de las libertades"* (art. 15). Por otro lado, no establece la necesidad de incluir un control judicial o independiente para todos los casos, sino que lo deja librado a la *"naturaleza del procedimiento o del poder de que se trate"*. De esta manera, la Convención confía la protección de las salvaguardas a los países mientras la enumeración de los poderes sí está incluida en el documento. Esta asimetría puede no resultar nociva en países como los europeos, en donde existe una tradición de respeto a la legalidad y los derechos de las personas. Sin embargo, en países como los de nuestra región puede servir como vía libre para abusos y malas prácticas, al carecer de una tradición robusta en la defensa de derechos.

- Varias de las disposiciones de la Convención apuntan hacia una disminución en la transparencia, al promover que los países aseguren el secreto de los procedimientos de conservación rápida de datos informáticos (art. 16 inc.3), obtención real de datos de tráfico (art. 20 inc. 3) o interceptación de datos de contenido (art. 21 inc.3). De esta manera la garantía de notificar al individuo que está siendo sometido a vigilancia o investigación puede ser limitada o suspendida, según el caso. Si bien es cierto que a veces es necesario que la persona no sepa que está siendo investigado a fin de no frustrar la investigación, hubiera sido deseable que se hubieran delimitado específicamente aquellos casos o haber establecido un plazo para mantener el secreto.

- Al momento de determinar quién es el autorizado para solicitar las medidas contempladas, el Convenio sólo habla de "autoridad competente", sin dejar en claro qué entiende por tal. Esto puede ser riesgoso para ciertas facultades sobre las cuales todavía hay discusión acerca

[13] Los datos de tráfico identifican a las comunicaciones que se realizan e incluyen: ubicación del equipo desde donde se realiza la comunicación, horario, duración, destinatario, entre otras.

de quién es el habilitado para ejercerlo. Pensemos en la solicitud de datos de tráfico. Algunos afirman que dichos datos no son tan comprometedores como los datos de contenido y por eso no se requiere una orden judicial para obtenerlos. De esta manera, el fiscal está autorizado para pedirlos en forma directa. Sin embargo, en la actualidad resulta claro que los datos de tráfico son tan o más reveladores de nuestra vida personal que los datos de contenido. De esta manera, requieren la más alta protección por parte de la legislación, lo cual incluye la necesidad de una orden judicial para su acceso. Este requisito no es establecido por la Convención y así se perdió la oportunidad para fortalecer las garantías para las personas.

- La cooperación internacional plantea cuestiones sensibles en materia de soberanía y jurisdicción, ya que puede implicar la obligación para los estados de entregar información de sus ciudadanos a terceros países. Es por eso que la regulación sobre este tema debe ser realizada con sumo cuidado para evitar poner en riesgo la privacidad de los ciudadanos frente a posibles abusos de otros estados. En este sentido, no debe soslayarse que varios de los países que son parte de la Convención de Budapest no cuentan con legislación sobre protección de datos personales y por ende carecen de garantías adecuadas para asegurar un manejo legítimo de la información recibida. Es por ello que no debe analizarse de manera aislada el Convenio sino en conjunto con otras disposiciones que autorizan la transferencia de datos únicamente a aquellos países que cuenten con un nivel suficiente de protección de datos personales.

- Otro aspecto polémico surge de la autorización que el Convenio otorga a un estado para que acceda a datos almacenados en otro país, sin pedir autorización a éste último, en caso de que haya obtenido el consentimiento de la persona que está *"legalmente autorizada a revelarlos por medio de ese sistema informático"* (art. 32). La ambigüedad de este concepto fue motivo de diversas controversias. Rusia se negó a firmar el tratado en base a que, según su consideración, esta disposición violaba la soberanía de los países, ya que únicamente bastaba el consentimiento del proveedor del servicio para que los datos puedan ser transferidos al país extranjero . Esta interpretación fue rechazada por el Comité del Convenio, que sostuvo en una nota explicativa que el proveedor del servicio no podía dar un consentimiento válido, ya que no es el controlador o el titular de los datos[14]. Sin embargo, esta interpretación no soluciona todos los problemas, ya que por más que por hipótesis se consiga el acuerdo del titular, el gobierno del estado seguiría sin ser notificado de aquel acceso. De esta manera, un supuesto tan sensible para la soberanía de los estados se encuentra insuficientemente regulado en el Convenio y de esa forma no puede cumplir un papel eficaz al momento de evitar interpretaciones abusivas o de mala fe sobre su aplicación.

[14] Comité de la Convención de Cibercrimen (2014). T-CY Nota explicativa No. 3: Acceso Transfronterizo a Datos (Articulo 32). Estrasburgo, Consejo de Europa, pag. 7, disponible en http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY%282013%297REV_GN3_transborder_V12adopted.pdf (último acceso: 29/01/17)

- Debido al año de su sanción (2001) el convenio se refiere principalmente a los términos de la cooperación entre estados. De esta manera, no aborda de manera adecuada los supuestos de cooperación entre un estado y una empresa privada. Estos casos son conocidos bajo la etiqueta de "cooperación asimétrica" y actualmente constituyen una forma muy utilizada para la obtención de prueba digital, debido a la proliferación de los servicios de computación en la nube. En estos casos, la cooperación está basada en protocolos establecidos por las empresas, a los cuales las autoridades deben ajustarse para poder ver satisfecha su solicitud. Esta situación hace que la entrega de datos quede sujeta a los criterios de las compañías, los cuales no son transparentes y no cuentan con mecanismos de rendición de cuentas, como los que habitualmente poseen las regulaciones surgidas de las autoridades públicas. Así, el Convenio se vuelve un instrumento inefectivo para lidiar con este fenómeno y se pierde la oportunidad de establecer una regulación más estricta sobre los acuerdos entre gobiernos y empresas privadas en términos de transparencia, publicidad y responsabilidad.

V. Conclusiones

En definitiva, el Convenio de Budapest resulta un instrumento que pretende abordar de manera integral el fenómeno del cibercrimen. Es por ello que se ocupa de establecer las conductas que deben ser consideradas como delitos así como los poderes y facultades que las autoridades poseen para investigarlos. Sin embargo, dicho tratado no ha dedicado el mismo detalle a establecer las garantías necesarias para que los individuos vean respetada su intimidad y su información personal. Asimismo, varios de los conceptos incluidos adolecen de serios problemas de ambigüedad, lo cual habilita a que autoridades sin un fuerte compromiso democrático puedan utilizarlos para restringir los derechos de sus ciudadanos. En este sentido, si bien existe un reporte explicativo[15] que intenta solucionar estos inconvenientes, no son más que recomendaciones y por ende la implementación final quedará en manos exclusiva de los estados. Por otro lado, el año de su sanción (2001) impide que haya un tratamiento adecuado de fenómenos que actualmente poseen gran relevancia como la prueba almacenada en la nube y la cooperación entre empresas y estados.

Así, la situación de los países de la región dependerá de su relación con el Convenio de Budapest. Aquellos que no están adheridos al tratado, deberían realizar un debate previo interno con la participación de la mayor cantidad de perspectivas posibles, a fin de evaluar cuidadosamente los pros y contras de una eventual incorporación a la Convención. En dicha evaluación, no debería considerarse a la seguridad y la defensa de los derechos como ideas contrapuestas sino como formando parte una de la otra. Además, debería analizarse el actual funcionamiento de la práctica vigente para ver

[15] La traducción al español del reporte explicativo de la Convención de Budapest se encuentra disponible en https://rm.coe.int/16802fa403 (último acceso: 07/02/2018).

efectivamente cuáles son los aspectos que necesitan mejora, sobre todo en materia de cooperación internacional.

Por otro lado, en los países que ya son parte del Convenio, el esfuerzo debería estar enfocado en su implementación. En ese sentido, la tarea es establecer de manera más detallada las garantías y salvaguardas que están ausentes en el texto de la Convención. Para ello, no debe perderse de vista las normas de la Constitución, del sistema interamericano y de protección de datos personales que sirven para delinear las defensas que las personas deben tener a fin de que las prácticas de investigación de los gobiernos no desemboquen en una violación de la privacidad, la libertad de expresión y demás derechos en juego.