C.R. & F. ROJAS
ABOGADOS

Fundado en 1900

NEWSLETTER

Agosto 2022 No. 2

Protocolo Adicional Segundo al Convenio de Budapest sobre Ciberdelincuencia

La Paz

Calle Federico Zuazo 1598, Edificio Park Inn
Piso 11

(+591 - 2) 211 3165
(+591 - 2) 231 3737

Santa Cruz

Avenida San Martín 155, Edificio Ambassador Business Center
Piso 19

(+591 - 3) 337 7474

www.rojas-lawfirm.com

Protocolo Adicional Segundo al Convenio de Budapest sobre Ciberdelincuencia

La pandemia por Covid-19 no solo ha puesto en evidencia la necesidad y el crecimiento en el uso de nuevas tecnologías para, por ejemplo, realizar tareas diarias tan básicas como acceder a la educación, adquirir productos y servicios en línea, comunicarnos con nuestro entorno familia, social, laboral, etc.

El uso de las nuevas (y no tan nuevas) tecnologías ha abierto una puerta a grupos de delincuencia organizada a nivel mundial en sectores tan diversos como la explotación sexual, tráfico de drogas, contrabando y. terrorismo.

Este protocolo mejora y complementa el Convenio del Consejo de Europa sobre Ciberdelincuencia de Budapest de 23 de noviembre de 2001 y el Protocolo Adicional Primero del mismo, firmado en Estrasburgo el 28 de enero de 2003.

Además de ser el primer tratado internacional en la materia, sigue siendo uno de los principales textos sobre cooperación internacional con la finalidad de perseguir a nivel penal y luchar efectivamente contra el ciberdelito transfronterizo.

El Segundo Protocolo Adicional al Convenio de Budapest sobre Ciberdelincuencia, según la Ministra de Justicia de Italia Marta Cartabia, responde a la necesidad de una cooperación mayor y más eficaz entre los Estados Miembros, otorgando la posibilidad de que los proveedores de servicios puedan facilitar los datos en su posesión a las autoridades competentes de otros países a efectos de responder oportunamente a la aclaración de los delitos mencionados. Distintos países latinoamericanos están considerando adherirse a éste.

Existe una serie de características comunes en los procesos de adhesión de los países latinoamericanos, como ser Argentina, Brasil, Chile, Colombia y México, incluyendo celeridad en la discusión de leyes y decretos, falta de transparencia, falta de participación de sectores relevantes y el uso de la necesidad de adecuación al Convenio de Budapest para promover reformas integrales de la legislación penal y procesal penal vigente. Como consecuencia, las reformas han puesto en

riesgo el ejercicio de derechos ciudadanos, tales como el derecho a la intimidad, el derecho a la protección de datos personales y el debido proceso.

Este Instrumento, al buscar establecer procedimientos que buscan reforzar la cooperación internacional, y al permitir el acceso de las fuerzas de seguridad a los datos de la ciudadanía, plantea una serie de importantes retos en relación a derechos humanos y libertades fundamentales.

En este entendido, Electronic Frontier Foundation y Al Sur[1] han manifestado preocupaciones y consideraciones respecto a los derechos humanos y estrategias específicas de mitigación.

Entre las principales preocupaciones se destacan las siguientes:

- Las normas más invasivas del Protocolo crean nuevos mecanismos que permiten a las autoridades competentes acceder a los datos con mayor rapidez y facilidad.
- La legalidad y la legitimidad de las investigaciones dependen del respeto de las garantías procesales penales, de la normativa sobre protección de datos y de la legislación internacional sobre derechos humanos.
- Garantizar los derechos en dichas investigaciones, cualquier injerencia en el derecho a la intimidad basada en una legislación accesible al público que sea precisa y no discriminatoria, que la injerencia sea legítima, necesaria y proporcionada es igualmente difícil.
- Asegurar que el acceso a los datos y su intercambio están autorizados por una autoridad judicial competente, imparcial e independiente, es tarea difícil.
- Garantizar que prevalecen los derechos al debido proceso, que se aplican mecanismos idóneos de supervisión y respeto a la inmunidad y privilegios, también lo es.

El artículo 7, párrafo 2, por ejemplo, obliga a las Partes a adoptar medidas legislativas para autorizar a los proveedores de servicios a responder a los requerimientos de datos de los abonados en respuesta a una orden en virtud del artículo 7, párrafo 1. Esto significa que si una ley nacional en el territorio donde se encuentra el proveedor de servicios les impide responder voluntariamente a las solicitudes de datos de los abonados sin las salvaguardias apropiadas—como un requisito de motivo razonable y/o una orden judicial—los Estados están ahora obligados a eliminar esas salvaguardias legales para los requerimientos directos transfronterizos.

En este sentido, Electronic Frontier Foundation y Al Sur sugieren una serie de salvaguardias[2] que los Estados, y los responsables de la toma de decisiones, deberían tener en cuenta al momento de promover la adhesión al Segundo Protocolo Adicional al Convenio de Budapest sobre Ciberdelincuencia:

- Requerir una autorización judicial previa también para acceder a los datos que no se consideran como contenido de las comunicaciones, incluyendo a los metadatos y a los datos relativos a abonados;
- Exigir una base probatoria clara para la solicitud de datos; - Basar la autorización judicial previa e independiente en una sólida demostración de que la medida de investigación que se contempla aportará pruebas de un delito grave;
- Establecer una supervisión reguladora independiente y eficaz del funcionamiento general del régimen transfronterizo, incluso mediante auditorías, controles aleatorios e informes anuales;
- Informar a los usuarios sobre el acceso de los gobiernos a sus datos personales, garantizar mecanismos efectivos de reparación y suficiente información para evaluar cualquier impacto en sus derechos humanos y libertades;
- Requerir la presentación de informes anuales de transparencia por parte del Estado sobre el volumen, la naturaleza y el alcance de las demandas de acceso a datos enviadas dentro y fuera de las fronteras, así como sobre las demandas de datos recibidas de otros Estados.

- Adoptar medidas legales que garanticen que las solicitudes de mordaza (solicitudes de confidencialidad y secreto) no se invocan de forma inapropiada cuando las fuerzas de seguridad solicitan el acceso a los datos;
- Garantizar explícitamente que los marcos legales nacionales reconozcan los datos biométricos como categóricamente personales sensibles en todos los casos, que deben ser tratados con los más altos niveles de protección.

Una vez más apreciamos la urgente necesidad de contar con mecanismos internos (leyes específicas, regulaciones detalladas y salvaguardas a los derechos fundamentales contemplados en la Constitución) que permitan, no solo hacer frente a abusos y posibles injerencias, sino también regular de forma adecuada y armónica con la legislación internacional, aquellos derechos fundamentales relativos a la privacidad de datos, intimidad y todos los derechos inherentes a la persona y la decisión sobre el uso, almacenamiento, distribución y publicación de sus datos, que permitan a los ciudadanos ejercer los derechos ARCO.

1. La Electronic Frontier Foundation es la principal organización sin ánimo de lucro dedicada a defender las libertades civiles en el mundo digital. Fundada en 1990, la EFF defiende la privacidad de los usuarios, la libertad de expresión y la innovación a través de litigios de impacto, análisis de políticas, activismo de base y desarrollo tecnológico. La misión de la EFF es garantizar que la tecnología apoye la libertad, la justicia y la innovación para todos los pueblos del mundo. "Al Sur" es un consorcio de organizaciones que trabajan en la sociedad civil y en el ámbito académico en América Latina y que buscan con su trabajo conjunto fortalecer los derechos humanos en el entorno digital de la región.
2. Evaluando el nuevo Protocolo al Convenio sobre Ciberdelincuencia en América Latina. https://www.alsur.lat/sites/default/files/2022-05/Guide-ES_Second%20Additional%20Protocol%20to%20the%20Cybercrime%20Convention%20in%20Latin%20America.pdf

Paula Bauer
C.R. & F. ROJAS ABOGADOS

El presente artículo no se trata de un análisis, es un breve comentario sobre la norma legal vigente en Bolivia

Anteriores Boletines

- Decisión No. 897 Lineamientos para la Protección de los Derechos de los Usuarios de Servicios de Telecomunicaciones

- Bolivia, un reto de país bisagra