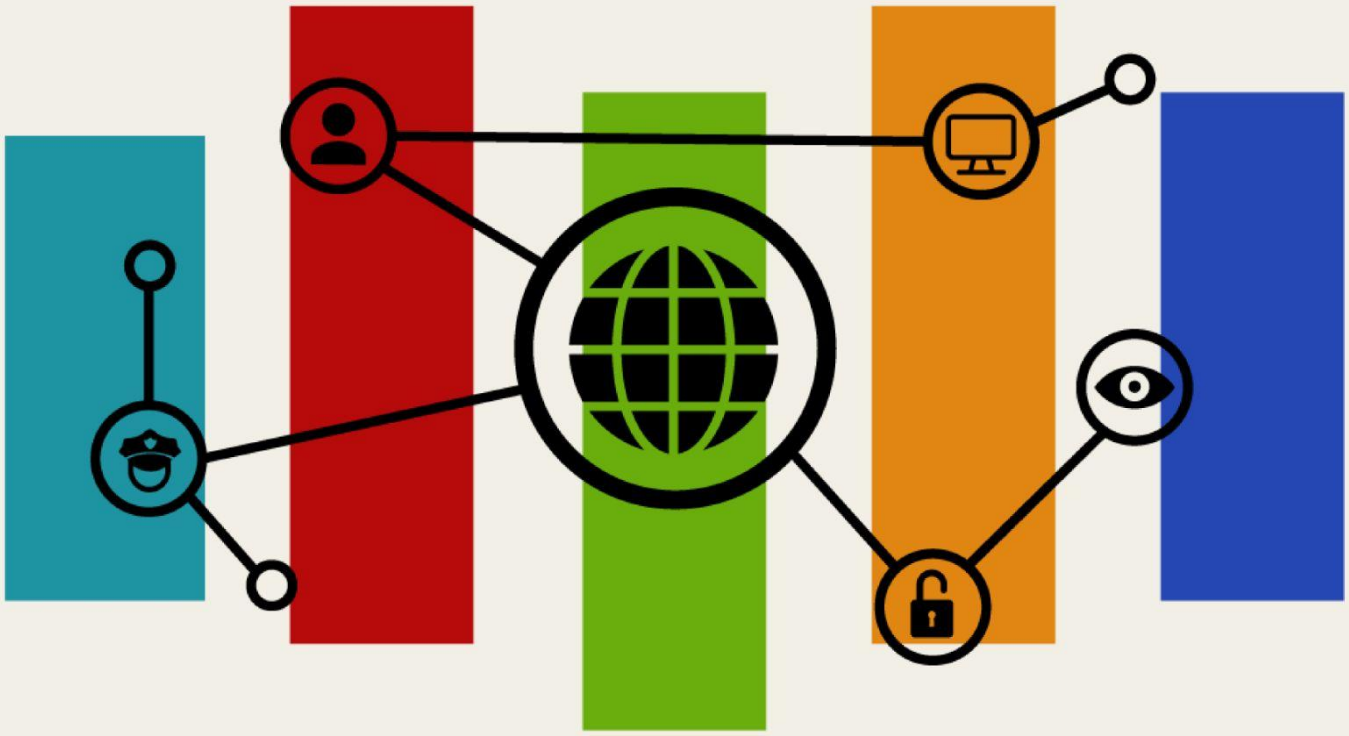


Evaluando el nuevo Protocolo al Convenio sobre Ciberdelincuencia en América Latina

Preocupaciones, consideraciones respecto a los derechos humanos y estrategias de mitigación

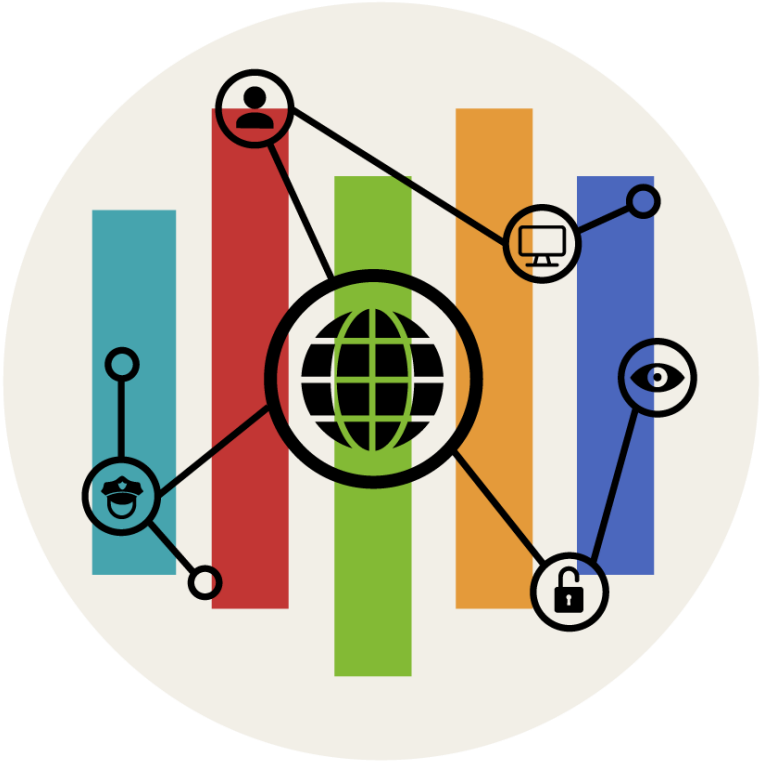
ELECTRONIC FRONTIER FOUNDATION

AlSur

Autor: Veridiana Alimonti
Coloboradores: Al Sur

Esta guía fue revisada por Katitza Rodríguez, Directora de Políticas de Privacidad Global de la EFF, y editada por Karen Gullo, Especialista en Relaciones con los Medios de Comunicación. El responsable de traducciones de la EFF, Carlos Wertheman, tradujo la guía al español. La directora de proyectos de ingeniería y diseño de la EFF, Kim Carlson, junto con el director de arte de la EFF, Hugh D' Andrade, dieron formato a esta guía. Artemis Schatzkin, ingeniera de la EFF, trabajó en el sitio web de Necessary & Proportionate para alojar esta guía.

Consulta este informe en línea:
https://necessaryandproportionate.org/files/protocol-cybercrime-convention-latam-es.pdf



Evaluando el nuevo Protocolo al Convenio sobre la Ciberdelincuencia en América Latina

Preocupaciones, consideraciones respecto a los derechos humanos y estrategias de mitigación

Veridiana Alimonti
Directora Asociada de Políticas en América Latina

Mayo de 2022

Introducción

El Protocolo adicional segundo al Convenio sobre la Ciberdelincuencia (en adelante "el Protocolo") relativo a la cooperación reforzada y la revelación de pruebas electrónicas pretende establecer nuevas normas internacionales que regulen aspectos de la actuación policial y la investigación penal a escala mundial[1]. El Protocolo fue adoptado por el Consejo de Europa (CdE) en noviembre de 2021[2]. Ahora y en los próximos meses, varios países de todo el mundo, especialmente aquellos que son parte del actual Convenio sobre la Ciberdelincuencia del CdE, están llevando a cabo o probablemente llevarán a cabo debates nacionales para evaluar su adhesión y una posible implementación del Protocolo en su marco jurídico nacional. Los países de América Latina que han pasado a formar parte del Convenio de Budapest sobre la Ciberdelincuencia de 2001 pueden adherirse al Protocolo[3].

Abierto a la firma el 12 de mayo de 2022, el Protocolo establece varios procedimientos para mejorar la cooperación internacional. Entre estas medidas se encuentran:

- Asistencia mutua en situaciones de emergencia.
- Revelación rápida de los datos informáticos almacenados en caso de emergencia.
- Cooperación entre autoridades para la revelación de datos informáticos almacenados.
- Los procedimientos que refuerzan la cooperación directa con los proveedores de servicios en el territorio de la otra Parte.

La presente guía pretende ayudar a las partes interesadas en los debates nacionales sobre una posible adhesión al Protocolo. Destaca que el Protocolo tiene considerables puntos débiles desde el punto de vista de los derechos humanos que deberían llevar a los países a reflexionar cuidadosamente sobre la pertinencia de ratificarlo, y que ameritan una consideración exhaustiva dentro de los debates nacionales sobre el Protocolo. Esta guía se centra en las medidas de cooperación directa con los proveedores de servicios y en las garantías de derechos humanos y protección de datos del Protocolo

Al convertirse en Parte del Protocolo, los países latinoamericanos elegibles implementarán estas nuevas facultades de acceso transfronterizo a los datos en su marco nacional. Los Estados Parte se basarán, entonces, en dichas normas cuando busquen datos en el extranjero y también se atendrán a sus condiciones y obligaciones cuando reciban solicitudes de autoridades extranjeras que sean Partes en el acuerdo.

[1] El texto completo del Protocolo adicional segundo al Convenio sobre la Ciberdelincuencia está disponible en https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224
[2] Ver más en https://www.coe.int/en/web/cybercrime/-/second-additional-protocol-to-the-cybercrime-convention-adopted-by-the-committee-of-ministers-of-the-council-of-europe
[3] En esta guía, los Estados Parte, las Partes y los signatarios se refieren a los Estados que se han adherido a un tratado o acuerdo internacional.

Esta guía ofrece una visión crítica del Protocolo, centrándose principalmente en los artículos 7, 13 y 14, y destaca las medidas de mitigación en caso de su adopción. La guía se divide en tres secciones: (**I**) Antecedentes del Protocolo; (**II**) Principales preocupaciones, incluyendo los posibles impactos negativos en los marcos de privacidad latinoamericanos; (**III**) Evaluación de la adhesión y mitigación de las debilidades. La guía tiene en cuenta los desafíos particulares de América Latina en el cumplimiento de las salvaguardias de los derechos humanos y el Estado de Derecho, y considera los marcos legales sobre la protección de datos personales y el acceso del gobierno a los datos de las comunicaciones en múltiples países latinoamericanos[4].

[4] Véase investigaciones anteriores sobre el acceso de los gobiernos a los datos en los países de América Latina consideradas en esta guía en https://necessaryandproportionate.org/country-reports/

I. Antecedentes del Protocolo

El nuevo acuerdo internacional es el Protocolo adicional segundo al Convenio del CdE sobre la Ciberdelincuencia, también conocido como Convenio de Budapest, que se abrió a la firma en 2001. El Convenio de Budapest es un amplio acuerdo internacional sobre ciberdelincuencia que establece obligaciones de derecho penal y procesal sustantivo para armonizar la legislación penal y mejorar la cooperación en las investigaciones que trascienden las fronteras. Fue el primer tratado internacional destinado a abordar la ciberdelincuencia y constituye el tratado sobre ciberdelincuencia más ampliamente ratificado en la actualidad, con 66 Estados Parte y más de 20 Estados y organizaciones observadores[5]. Aunque el Convenio contiene normas sobre el acceso transfronterizo a los datos y la cooperación internacional, la mayoría de sus disposiciones se refieren a la legislación y a las investigaciones sobre ciberdelincuencia a nivel nacional. Por su parte, el Protocolo se centra en el refuerzo de la cooperación internacional entre las autoridades y con los proveedores de servicios en otro territorio. El Protocolo incluye varias medidas legales, que van desde la asistencia mutua en situaciones de emergencia, la revelación rápida de datos informáticos almacenados en caso de emergencia y la cooperación entre autoridades para la revelación de datos informáticos almacenados. También incluye procedimientos que refuerzan la cooperación directa con los proveedores de servicios en el territorio de otra Parte, incluidas las medidas para que las autoridades competentes accedan a los datos personales en poder de un proveedor en otro territorio.

El Convenio de Budapest de 2001 ha sido bastante influyente en América Latina[6], actuando como directriz para los países que desarrollan una legislación nacional integral contra la ciberdelincuencia, y como marco para la cooperación internacional entre los Estados Parte de este tratado. El Protocolo tiene un potencial similar y un atractivo adicional. Dado que muchas autoridades competentes pueden querer acceder a pruebas electrónicas a través de las fronteras, es probable que los Estados busquen la adhesión al Protocolo debido a sus novedosas normas de cooperación. Solo los Estados de América Latina que ya son parte del Convenio de Budapest de 2001 pueden adherirse al Protocolo segundo[7]. Hasta la fecha, son Argentina, Chile, Costa Rica, Colombia, República Dominicana, Panamá, Paraguay y Perú. Brasil y México fueron invitados a ser partes y han actuado como observadores, siendo que la adhesión de Brasil al Convenio de Budapest ha sido aprobada por el Congreso en diciembre de 2021.

A pesar de los antecedentes de fuerte compromiso del CdE con la participación de las partes interesadas, el proceso de redacción del Protocolo por parte del Comité de Ciberdelincuencia del CdE (T-CY) estuvo fuertemente influenciado por los agentes de

[5] Véase en https://www.coe.int/en/web/cybercrime/parties-observers
[6] Véase Bruna Martins dos Santos. Derechos Digitales. Budapest Convention on Cybercrime in Latin America: a brief analysis of adherence and implementation in Argentina, Brazil, Chile, Colombia and Mexico, 2022.
[7] Artículo 16 del Protocolo e Informe Explicativo del Protocolo, párrafo 294. Disponible en https://rm.coe.int/1680a49c9d

seguridad pública y de las fuerzas del orden[8]. Los grupos de derechos humanos y digitales, los abogados defensores e incluso los reguladores de la protección de datos[9] fueron en gran medida marginados durante el proceso de redacción, lo que fue señalado por las organizaciones de la sociedad civil[10]. El texto resultante es una expresión de este proceso desigual, con salvaguardias obligatorias de derechos humanos que no son tan sólidas como las obligaciones que facilitan el acceso policial transfronterizo a los datos personales. Los países que evalúen la posibilidad de adherirse al Protocolo deben tener en cuenta sus deficiencias en relación con su contexto nacional y el marco jurídico aplicable, a fin de identificar adecuadamente las lagunas en la protección de los derechos humanos y examinar las preocupaciones. La siguiente sección destaca las principales preocupaciones que deben tenerse en cuenta.

En síntesis, agrupamos estas preocupaciones en cuatro categorías: (i) el debilitamiento de los derechos y las salvaguardias mediante requerimientos directos de cooperación para los proveedores de servicios en los territorios de los Estados Parte; (ii) la concepción errónea sobre la información relativa a abonados por parte del Protocolo y su influencia negativa en los marcos jurídicos latinoamericanos en materia de privacidad; (iii) el desequilibrio entre las facultades obligatorias de aplicación de la ley y las salvaguardias prescindibles u opcionales en materia de derechos humanos; (iv) las salvaguardias más débiles en materia de protección de datos en comparación con otras normas internacionales ya establecidas.

[8] Katitza Rodríguez, Tamir Israel. Global Law Enforcement Convention Weakens Privacy & Human Rights, 8 de junio de 2021.
https://www.eff.org/deeplinks/2021/06/global-law-enforcement-convention-weakens-privacy-human-rights

[9] El Consejo Europeo de Protección de Datos (CEPD), en las presentaciones del organismo a las consultas del TC-Y para el proyecto de texto del Protocolo, ha subrayado repetidamente la importancia de involucrar a las autoridades de protección de datos en el proceso de redacción del Protocolo. Véase la contribución del CEPD en noviembre de 2019
https://www.eff.org/deeplinks/2021/07/council-europes-actions-belie-its-pledges-involve-civil-society-development-cross y la declaración del CEPD en febrero de 2021
https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-022021-new-draft-provisions-second-additional_en

[10] Véase, por ejemplo, la Carta conjunta de las organizaciones de la sociedad civil al Presidente del Comité de Ministros del Consejo de Europa. 31 de mayo de 2021.
https://www.eff.org/files/2021/06/07/final_letter_-_council_of_europe-final.pdf . Véase también Karen Gullo, Katitza Rodríguez. Council of Europe's Actions Belie its Pledges to Involve Civil Society in Development of Cross Border Police Powers Treaty. 22 de julio de 2021.
https://www.eff.org/deeplinks/2021/07/council-europes-actions-belie-its-pledges-involve-civil-society-development-cross

II. Principales preocupaciones

Los Tratados de Asistencia Legal Mutua (MLAT) han proporcionado tradicionalmente el marco principal para la cooperación gubernamental en investigaciones criminales transfronterizas. Los MLAT suelen ser acuerdos bilaterales, negociados entre dos países, con salvaguardias integradas. Varios Estados afirmaron que el proceso de los MLAT es lento, lo que provoca retrasos en las investigaciones penales[11]. Las normas más invasivas del Protocolo tratan de responder a estas reclamaciones creando nuevos mecanismos que permitan a las autoridades competentes acceder a los datos con mayor rapidez y facilidad.

Sin embargo, los esfuerzos por lograr una mayor eficacia en el acceso a los datos personales en las investigaciones penales transfronterizas deben basarse siempre en una sólida protección de los derechos humanos. 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. Si las investigaciones transfronterizas son un reto, garantizar los derechos humanos en dichas investigaciones es igualmente difícil. ¿Cómo garantizar que cualquier injerencia en el derecho a la intimidad se base en una legislación accesible al público, precisa y no discriminatoria, y que la injerencia sea legítima, necesaria y proporcionada? ¿Cómo asegurarse de que el acceso a los datos y su intercambio están autorizados por una autoridad judicial competente, imparcial e independiente? ¿Cómo asegurarse de que prevalecen los derechos del debido proceso, se aplican los mecanismos de supervisión y se respetan la inmunidad y los privilegios?

Cualquier nuevo régimen para agilizar el acceso transfronterizo debe preservar las salvaguardias cruciales necesarias para defender los derechos humanos. Los MLAT, por ejemplo, suelen implicar:

- Un mecanismo para solicitar asistencia para acceder a los datos almacenados en otro país;
- Una Autoridad Central que evalúa y responde a las solicitudes de asistencia de los Estados extranjeros o deniega las solicitudes que son contrarias a los derechos humanos;
- Una base legal en la legislación nacional que autorice a la Autoridad Central a obtener datos en nombre del Estado requirente ;
- La obligación de las Autoridades Centrales de basarse en los poderes de búsqueda nacionales (y estar obligadas por las protecciones nacionales de la privacidad que los acompañan) cuando obtengan datos en respuesta a una solicitud.
- Una evaluación por parte de los Estados de la compatibilidad del acuerdo MLAT y del sistema jurídico de la otra Parte con su respectivo marco jurídico nacional para garantizar que se respeten los valores fundamentales y las normas de derechos humanos.

[11] Vease en https://www.eff.org/deeplinks/2015/12/reforms-abound-cross-border-data-requests

Desgraciadamente, el artículo 7 del Protocolo se queda corto a la hora de ofrecer garantías efectivas de derechos humanos, aunque el artículo 8 mantiene algunas de las garantías integradas en el sistema de los MLAT.

Aunque nuestro análisis a continuación se centra predominantemente en el artículo 7 del Protocolo, observamos que el artículo 6 implica intereses y preocupaciones similares en materia de privacidad y derechos humanos. Ambos artículos prevén la transferencia directa de datos personales de los proveedores de servicios situados en el territorio de un Estado Parte del Protocolo a las autoridades competentes (e.j., la policía, los fiscales) de otro Estado Parte.

(a) Los defectos inherentes al artículo 7

El artículo 7, párrafo 1, del Protocolo obliga a los Estados firmantes a adoptar medidas legislativas para facultar a sus autoridades competentes[12] a requerir directamente la revelación de la información relativa a abonados que esté en posesión o control de un proveedor de servicios situado en el territorio de otra Parte—lo que elimina los mecanismos clave de escrutinio de los derechos humanos.

Conforme al mecanismo por defecto del artículo 7, las autoridades del Estado Parte en el que se encuentra el proveedor no desempeñarán ninguna función de "verificación" y, por tanto, no lograrán rechazar una solicitud específica de asistencia si entra en conflicto con el marco de derechos humanos de su Estado. Según este mecanismo, las autoridades policiales de un Estado que estén facultadas por la legislación nacional para ordenar a los proveedores de servicios que revelen información sobre los abonados podrán presentar un requerimiento directo para los proveedores ubicados en otro Estado Parte, siguiendo únicamente la norma jurídica del Estado requirente. Esto significa que los requerimientos podrán emitirse sin ningún tipo de supervisión por parte de una autoridad judicial u otra autoridad independiente si no son requisitos en el marco nacional de la Parte requirente.

El artículo 7, párrafo 2, también 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.

[12] El artículo 3, párrafo 2(b) del Protocolo define la "autoridad competente" como una autoridad judicial, administrativa o de otro tipo encargada de hacer cumplir la ley que esté facultada por el derecho interno para ordenar, autorizar o llevar a cabo la ejecución de medidas contempladas en el presente Protocolo a efectos de la obtención o la presentación de pruebas con relación a investigaciones o procedimientos penales específicos.

Los requerimientos a los proveedores de servicios en virtud del apartado 1 del artículo 7 se presentan en el texto del Protocolo como "órdenes" ("orders" en el texto inglés original), que son vinculantes a nivel nacional, aunque no son directamente ejecutables por las autoridades extranjeras requirentes, dada su aplicación transfronteriza. En principio, los proveedores de servicios siguen teniendo margen para rechazar estos requerimientos directos, pero el hecho de que su cumplimiento puede ser ejecutado mediante procedimientos para obligar a la presentación de la información ("dar efecto a una orden") establecidos en el artículo 8[13], u por otra forma de asistencia mutua, probablemente disuadirá a los proveedores de rechazar dichos requerimientos. De hecho, en virtud del artículo 7, los proveedores de servicios ni siquiera reciben suficiente información para evaluar o procesar adecuadamente un requerimiento para identificar las circunstancias que son incompatibles con los derechos humanos y las libertades fundamentales.

De esta manera, el Protocolo puede crear asimetrías injustificables en la legislación nacional. Por ejemplo, en virtud de la definición excesivamente amplia de "autoridad competente" del Protocolo[14], *cualquier* autoridad administrativa o policial facultada por su legislación nacional para emitir un requerimiento de datos relativo a abonados está facultada para hacerlo directamente a un proveedor de servicios situado en el territorio de otra Parte. En consecuencia, los requerimientos directos transfronterizos pueden emitirse sin ningún tipo de supervisión por parte de una autoridad judicial u otra autoridad independiente en la Parte requirente, lo que puede permitir a las autoridades extranjeras aplicar una base jurídica más permisiva y menos protectora de la privacidad para acceder a los datos de los abonados que lo que los agentes locales encargados de hacer cumplir la ley estarían obligados a hacer en virtud de la legislación local de la Parte requerida.

México: En 2016, la Segunda Sala de la Suprema Corte de Justicia de la Nación sostuvo que se requería una orden judicial para revelar datos retenidos que permitan identificar las comunicaciones, incluyendo la información relativa a abonados, y señaló que las autoridades deben especificar los objetivos y los períodos de tiempo, así como justificar la necesidad de la información buscada[15].

[13] El artículo 8, párrafo 1, exige a los Estados Parte que adopten medidas legislativas y de otro tipo que sean necesarias para facultar a sus autoridades competentes a dictar una orden al Estado Parte donde se encuentra el proveedor para que este pueda obligar a los proveedores de servicios locales a presentar los datos almacenados de los abonados y del "tráfico" que estén en posesión y control del proveedor. El artículo 8, párrafo 2, exige a la Parte requerida, donde se encuentra el proveedor, que adopte las medidas legislativas y de otro tipo que sean necesarias para dar efecto a la orden de la Parte requirente. Por lo tanto, si un proveedor de servicios no cumple un requerimiento directo en virtud del artículo 7, la Parte requirente puede solicitar la ejecución en virtud del mecanismo del artículo 8. Las Partes no pueden pretender la ejecución unilateral. Véase el Informe Explicativo del Protocolo, párrafo 117.

[14] Véase la nota 12 supra.

[15] Véase en https://www.internet2.scjn.gob.mx/red2/comunicados/comunicado.asp?id=4301

Chile: Los proveedores de servicios de Internet (ISP) chilenos exigen una autorización judicial previa como mejor práctica voluntaria a la hora de procesar los requerimientos de datos de los abonados nacionales[16]. El Código Procesal Penal del país permite una norma más protectora al exigir una orden judicial previa en todos los procedimientos que afecten, priven o restrinjan los derechos constitucionales de privacidad de un acusado o de un tercero.

Brasil: La Ley brasileña n. 12.965/2014 requiere una orden judicial antes de que los datos de las comunicaciones de los usuarios, como las direcciones IP, puedan ser revelados a los agentes encargados de hacer cumplir la ley. Sin embargo, las autoridades administrativas locales pueden solicitar directamente los datos de los abonados, como el nombre y la dirección, cuando la ley lo autorice específicamente.

En las consultas realizadas durante el proceso de redacción, la EFF, junto con organizaciones de la sociedad civil de Europa y América, incluidos grupos que forman parte de Al Sur, instó al CdE a eliminar el artículo 7 del proyecto de texto del Protocolo, permitiendo que el artículo 8 se convirtiera en la base jurídica principal por la que se accede a los datos de los abonados en contextos transfronterizos[17]. La Asociación Europea de Proveedores de Servicios de Internet (EuroISPA) hizo recomendaciones similares en sus propuestas[18]. El artículo 8 requiere la participación de las autoridades nacionales de la Parte requerida. De este modo, las autoridades de la Parte requerida pueden aplicar las normas contenidas en su propia legislación nacional al obligar la presentación de los datos de los abonados por los proveedores de servicios locales situados en su territorio. Aunque el artículo 8 no exige la supervisión judicial de las solicitudes policiales, los Estados con una fuerte protección de la privacidad pueden seguir confiando en sus propios tribunales cuando obliguen a un proveedor de servicios local a identificar a sus clientes. Cabe señalar que el artículo 8 ya prevé una solicitud de asistencia mutua rápida, mientras que los artículos 9 y 10 abordan la cooperación internacional en situaciones de emergencia, sin anular el papel de las autoridades nacionales de la Parte en la que se encuentra el proveedor.

El párrafo 9(a) del artículo 7 permite a las Partes reservarse el derecho a no aplicar el artículo 7 en su totalidad, pero solo en el momento de la firma o al depositar su

[16] Véase en https://www.derechosdigitales.org/wp-content/uploads/QDTD-2021.pdf . Véanse también las directrices de aplicación de la ley de las empresas de telecomunicaciones chilenas GTD (https://www.gtd.cl/normativa/privacidad-y-proteccion-de-datos-personales/requerimientos-de-informacio) y Claro (https://www.clarochile.cl/portal/cl/archivos_generales/politica-requerimientos-de-informacion-Marzo-de-2021_20210331.pdf).

[17] EFF, Derechos Digitales, EDRi, Fundación Karisma, CIPPIC, TEDIC. Privacy & Human Rights in Cross-Border Law Enforcement. Comentario conjunto de la sociedad civil a la Asamblea Parlamentaria del Consejo de Europa (PACE) sobre el Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia (CETS 185). 9 de agosto de 2021, p. 5. Disponible en https://www.eff.org/files/2021/08/17/20210816-2ndaddprotocol-pace-ver2-final.pdf

[18] Véanse, por ejemplo, las alegaciones de EuroISPA a la 4ª ronda (https://rm.coe.int/euroispa-s-comments-to-draft-provisions-2nd-add-protocol-final/168098bcab) y a la 6ª ronda de consultas (https://rm.coe.int/0900001680a25789).

instrumento de ratificación, aceptación o aprobación. Una Parte que se reserve el artículo 7 no podrá dictar requerimientos directos de cooperación en virtud del apartado 1 del artículo 7 a los proveedores de servicios en los territorios de otras Partes[19].

Por otra parte, el artículo 7 estipula **salvaguardias opcionales**, no exigidas por el texto, pero que pueden ser invocadas a través de las reservas y declaraciones de un Estado Parte. Se establecen en el artículo 7, párrafo 2(b); en el artículo 7, párrafo 5 (a) y (b); y en el artículo 7, párrafo 9(b). Las reservas solo se permiten en el momento en que un Estado se adhiere al Protocolo. En algunos casos, esta restricción también se aplica a las declaraciones. Por lo tanto, para presentar adecuadamente estas salvaguardias opcionales y su importancia, debemos considerar qué es la información relativa a abonados y por qué debemos preocuparnos por las circunstancias en las que puede acceder a ella la policía.

¿Qué cosa es la información relativa a abonados?

El Convenio de Budapest siempre ha promovido una distinción entre los "datos de tráfico" (equivalentes a los "metadatos") y la "información relativa a abonados", y los define por separado. La "información relativa al abonados" se define de forma bastante amplia en el apartado 3 del artículo 18 del Convenio de Budapest[20]. Como se señala en el Informe Explicativo del Convenio, la información relativa a abonados se necesita principalmente en dos situaciones específicas en el curso de una investigación penal: (i) para identificar qué servicios y medidas técnicas relacionadas ha utilizado o está utilizando el abonado, y (ii) para establecer la identidad de la persona en cuestión cuando se conoce una dirección técnica (por ejemplo, una dirección IP)[21]. El Informe Explicativo del Protocolo utiliza la definición de datos de los abonados del Convenio de Budapest para considerar que esta definición incluye tipos de información sobre la dirección IP[22]. El Protocolo también establece un nivel de protección inferior para el acceso transfronterizo a la información de los abonados en relación con las salvaguardias de cooperación internacional aplicadas a los datos de tráfico o al contenido de las comunicaciones.

[19] Véase el Informe Explicativo del Protocolo, párrafo 122.
[20] La disposición estipula que "[...] se entenderá por "datos relativos a los abonados" cualquier información, en forma de datos informáticos o de cualquier otro modo, que posea un proveedor de servicios y que se refiera a los abonados de sus servicios, diferentes de los datos relativos al tráfico o al contenido, y que permitan determinar: (a) el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el período de servicio; (b) la identidad, la dirección postal o situación geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso y los datos relativos a la facturación y al pago, disponibles en virtud de un contrato o de un acuerdo de prestación de servicio; (c) cualquier otra información relativa al lugar en que se encuentren los equipos de comunicación, disponible en virtud de un contrato o de un acuerdo de prestación de servicio".
[21] Véase el Informe Explicativo del Convenio de Budapest, párrafo 178.
[22] Informe Explicativo del Protocolo, párrafo 93.

¿Por qué es importante la información relativa a abonados?

Su dirección IP puede revelar a las autoridades qué sitios web visita y con quién se comunica. Puede revelar identidades en línea que de otro modo serían anónimas, sus contactos en las redes sociales e incluso, a veces, su ubicación física a través del GPS. La policía puede solicitar su nombre, los datos del suscriptor que vinculan su identidad con su actividad en línea, y eso puede usarse para crear un perfil policial muy detallado de sus hábitos diarios, y también puede proporcionar pistas relevantes sobre el contenido de sus comunicaciones. Incluso revelar una identidad asociada a un número de teléfono específico puede ser delicado, cuando podría, por ejemplo, revelar la fuente de un periodista. Las consecuencias de unas protecciones débiles a la hora de desvelar identidades por lo demás anónimas pueden ser nefastas. La falta de salvaguardias adecuadas, como en el caso del artículo 7 del Protocolo, supone una amenaza para la seguridad de los activistas, los defensores de los derechos humanos, los disidentes, los periodistas y las personas corrientes que pueden sufrir persecución y represalias por oponerse y criticar a los poderes arraigados.

Chile: En 2013, la Fiscalía formalizó una investigación contra Rodrigo Ferrari por cargos de usurpación de identidad como presunto autor de tres cuentas de Twitter que parodiaban al empresario Andrónico Luksic, dueño de un importante conglomerado empresarial en Chile. Los fiscales obtuvieron la dirección IP, el nombre de usuario y el correo electrónico de la cuenta de Twitter @losluksic. Luego, la empresa de telecomunicaciones VTR divulgó su nombre, DNI, número de teléfono y correo electrónico sin requerir ninguna autorización judicial. La fiscalía no pudo probar la conexión de Ferrari con las otras dos cuentas de Twitter, y la cuenta @losluksic (la única reconocida por Ferrari) no fue suficiente para proceder con una acusación de robo de identidad. Aunque finalmente se archivó el caso, Ferrari se arriesgó a pasar entre 61 y 540 días en la cárcel y se enfrentó a la presión de la fiscalía para declararse culpable y aceptar un acuerdo[23].

Más recientemente, la fiscalía de Chile trató de obtener todos los números de teléfonos móviles que se habían conectado a las antenas de las estaciones de metro de Santiago, donde los incendios marcaron el inicio de la revuelta social y las protestas del país en 2019. Al obtener los números de teléfonos móviles, sería posible identificar a sus propietarios ubicados en la zona de las protestas. Sólo una empresa de telecomunicaciones accedió a la petición directa y voluntaria del fiscal, mientras que otras requirieron una orden judicial. El carácter amplio y desproporcionado de la solicitud también debería ser objeto de un mayor escrutinio [24].

[23] Vea la entrevista con Rodrigo Ferrari en https://www.theclinic.cl/2016/09/22/554806/
[24] Véase en https://www.biobiochile.cl/noticias/ciencia-y-tecnologia/moviles-y-computacion/2020/01/08/afirman-que-wom-entrego-informacion-de-usuarios-durante-estallido-social-compania-se-defendio.shtml

Paraguay: En 2016, uno de los principales medios de comunicación paraguayos, ABC Color, reveló que funcionarios de inteligencia de las fuerzas militares accedieron ilegalmente a datos de una empresa de telecomunicaciones para identificar a una de sus periodistas que informaba sobre un caso de corrupción en el ejército, así como a sus posibles fuentes[25].

Brasil: A finales de 2020, los estudiantes de derecho que crearon las cuentas de Twitter Sleeping Giants Brasil y Sleeping Giants Rio Grande do Sul decidieron revelar públicamente sus identidades después de que un juez obligara a Twitter a revelar las direcciones IP y otros datos capaces de identificar a los propietarios de las cuentas. Antes de revelar sus identidades a la prensa, los estudiantes tomaron medidas para preservar su seguridad. Ambas cuentas de Twitter notifican a las marcas la presencia de sus anuncios en sitios web que difunden desinformación y discursos de odio. La demanda civil fue presentada por el Jornal da Cidade, un periódico que fue objeto de las cuentas de los Sleeping Giants. Se considera que el medio de comunicación difundió desinformación a favor de la campaña electoral del presidente Bolsonaro, fue incluido en una investigación del Congreso sobre la difusión de noticias falsas y sus piezas fueron verificadas y consideradas falsas en diferentes ocasiones[26].

Los tribunales y los organismos de derechos humanos entienden cada vez más que el acceso a algunas direcciones IP y otros identificadores en línea (un tipo de dato relativo a abonados en ciertas jurisdicciones) con el fin de identificar la actividad anónima en línea [27] puede revelar buena parte de la vida de las personas—incluidos detalles sensibles de sus intereses, creencias, relaciones y estilo de vida íntimo—y, por tanto, dicho acceso debe estar sujeto a sólidas protecciones.

Como ejemplo reciente, el Tribunal Europeo de Derechos Humanos, en el caso *Benedik contra Eslovenia*, sostuvo que se había producido una violación del derecho al respeto de la vida privada y familiar cuando la policía eslovena no obtuvo una orden judicial antes de acceder a la información de los abonados asociada a una dirección IP dinámica. Según

[25] Vea la cobertura mediática del caso en https://www.abc.com.py/edicion-impresa/notas/gobierno-uso-su-sistema-de-inteligencia-para-espiar-periodista-1511976.html y en https://www.abc.com.py/edicion-impresa/politica/fiscalia-ya-sabe-que-hubo-espionaje-a-equipo-telefonico-de-periodista-de-abc-1513518.html

[26] Vea las noticias sobre el caso en https://brasil.elpais.com/brasil/2020-08-25/acoes-judiciais-tentam-revelar-identidade-de-administrador-do-sleeping-giants.html , https://www1.folha.uol.com.br/colunas/monicabergamo/2020/12/sleeping-giants-sai-do-anonimato-em-entrevista-a-folha.shtml , y en https://olhardigital.com.br/2020/12/17/noticias/criadores-da-conta-sleeping-giants-brasil-revelam-suas-identidades/

[27] Utilizamos el término "anónimo" para referirnos a una actividad en línea no identificada directamente con respecto a la persona o personas implicadas—aunque puede implicar un identificador, como una dirección IP o un número IMEI, o ser identificable a través de otros medios disponibles o razonablemente susceptibles de ser utilizados para identificar a una persona física.

el Tribunal, la disposición legal utilizada por la policía eslovena para acceder a los datos de los abonados asociados a la dirección IP, sin obtener previamente una orden judicial, no había cumplido la norma del Convenio Europeo de Derechos Humanos de ser "conforme a derecho"[28].

Otras jurisdicciones también han reconocido la importancia del anonimato como componente del derecho a la intimidad. El Tribunal Supremo de Canadá, en particular, dijo en una sentencia que el anonimato de las personas en línea debe ser protegido cuando anuló la adquisición sin orden judicial de la identidad de un usuario por parte de la policía como inconstitucional, declarando:

> "[P]articularmente importante en el contexto del uso de Internet es la comprensión de la privacidad como anonimato. Debe reconocerse que la identidad de una persona vinculada a su uso de Internet da lugar a un interés de privacidad que va más allá del inherente al nombre, la dirección y el número de teléfono de la persona que se encuentra en la información del abonado. La información relativa a abonados, al tender a vincular determinados tipos de información con individuos identificables, puede implicar intereses de privacidad relacionados con la identidad de un individuo como fuente, poseedor o usuario de esa información. Un cierto grado de anonimato es una característica de gran parte de la actividad de Internet y, dependiendo de la totalidad de las circunstancias, el anonimato puede ser el fundamento de un interés de privacidad que involucra la protección constitucional contra el registro y la incautación irrazonables. En este caso, la solicitud de la policía de vincular una determinada dirección IP a la información de un suscriptor era, en efecto, una solicitud de vincular a una persona concreta con actividades específicas en línea. Este tipo de solicitud implica el aspecto del anonimato del interés de la privacidad informativa al intentar vincular al sospechoso con actividades en línea realizadas de forma anónima, actividades que han sido reconocidas en otras circunstancias como que implican intereses de privacidad significativos. . . La divulgación de esta información equivaldrá a menudo a la identificación de un usuario con actividades íntimas o delicadas realizadas en línea, normalmente en el entendimiento de que estas actividades serían anónimas. La solicitud de un agente de policía para que un ISP revele voluntariamente dicha información equivale a un registro."[29].

Lamentablemente, el Protocolo está en contradicción con estas tendencias. Permite los requerimientos directos transfronterizos de información relativa a abonados a los proveedores de servicios sin establecer un requisito de autorización independiente o judicial previa. En su lugar, considera la información de los abonados, *per se*, como una categoría de datos menos intrusiva para la privacidad.

---

[28] Véase la sentencia del TEDH en https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-182455%22]}.

[29] R. contra Spencer, 2014 SCC 43, 13 de junio de 2014. Además, el tribunal declaró que el "objeto de la búsqueda no era simplemente un nombre y una dirección de alguien que tenía una relación contractual con el ISP. Más bien, era la identidad de un abonado a Internet que corresponde a un uso particular de Internet." La decisión está disponible en https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do?r=AAAAAQAHc3BlbmNlcgE

Los Estados aún pueden modificar su código procesal penal o ley similar y exigir una autorización judicial previa para acceder a los datos relativos a abonados. Aunque no resolverá el problema cuando un Estado Parte extranjero solicite datos a los proveedores de servicios locales en virtud de las competencias del Protocolo, puede ayudar a aumentar el nivel de protección de la privacidad. La divulgación forzosa de hablantes anónimos solo debería producirse cuando se haya cometido un delito legalmente definido. E incluso en esos casos, deberían considerarse todos los derechos de un orador en línea antes de identificar a ese individuo en respuesta a una solicitud para hacerlo. Las autoridades judiciales, y no las empresas privadas, son las más indicadas para equilibrar el derecho de los ciudadanos a la expresión anónima con la necesidad de proporcionar un mecanismo para reparar los daños. Pero los sistemas judiciales solo pueden funcionar cuando un juez o un tribunal tiene la oportunidad de revisar las circunstancias antes de que se revele la identidad. Por lo tanto, para proteger la libertad de expresión y la privacidad de una persona, los proveedores de servicios solo deberían revelar la identidad de un usuario anónimo o seudónimo de su plataforma o servicio cuando reciban una orden judicial, concedida tras un proceso de revisión judicial previa[30].

El preocupante procedimiento estándar del artículo 7 y las salvaguardias opcionales a tener en cuenta

El Protocolo utiliza la distinción del Convenio de Budapest entre "datos de tráfico" e "información relativa a abonados" para incorporar un nivel inferior de protección de los datos de los abonados en el contexto de las solicitudes transfronterizas, permitiendo a la Parte requirente acceder a los datos con arreglo a sus propias normas jurídicas nacionales. Hace la preocupante suposición de que "la información de los abonados... no permite sacar conclusiones precisas sobre la vida privada y los hábitos diarios de los individuos en cuestión", como se señala en el Informe Explicativo del Protocolo[31]. El Protocolo considera los datos relativos a abonados como una categoría de información por naturaleza menos intrusiva que otros tipos de datos. Con ello, el acuerdo pasa por alto que desvelar la identidad de las personas asociada a sus actividades expresivas puede ser altamente sensible. También pasa por alto que la información de los abonados puede revelar datos de tráfico e incluso permitir inferencias sobre el contenido de las comunicaciones. Tal y como afirman los *13 Principios sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones*, estas categorías formalistas de datos como "contenido", "información relativa a abonados" o "metadatos" ya no son apropiadas para medir el grado de intrusión de la vigilancia de las comunicaciones en la vida privada y las asociaciones de las personas[32].

Según el procedimiento estándar del artículo 7, *cualquier* autoridad *competente de* la Parte requirente[33], de acuerdo con su legislación interna, puede emitir una orden

[30] Katitza Rodríguez. Comentários sobre anonimato y encriptación presentados al Relator Especial de las Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y de expresión, febrero de 2015. https://www.ohchr.org/Documents/Issues/Opinion/Communications/EFF.pdf
[31] Informe Explicativo del Protocolo, párrafo 92.
[32] Véase en https://necessaryandproportionate.org/principles/
[33] Véase la nota 12 supra para la definición de "autoridades competentes" del Protocolo.

exigiendo el acceso a la información de los abonados que esté en posesión o bajo el control de un proveedor de servicios situado en el territorio de otra Parte. Una posible vía para mitigar las asimetrías cuando las normas de la Parte requirente difieren de las aplicadas en el Estado requerido está prevista en **el artículo 7, párrafo 2(b). En virtud de este párrafo, una Parte puede declarar que los requerimientos emitidos a los proveedores de servicios en su territorio "deben ser dictados por un fiscal u otra autoridad judicial, o estar bajo su supervisión, o ser dictado bajo supervisión independiente".** Sin embargo, las Partes no pueden exigir la aprobación judicial independiente previa de los requerimientos extranjeros directos. Como se indica en el Informe Explicativo, una Parte que haga uso de esta declaración debe aceptar un requerimiento dictado por o bajo la supervisión de cualquiera de estas autoridades enumeradas, lo que incluye a los fiscales.

Si bien los Estados deben garantizar que los fiscales puedan desempeñar sus funciones sin intimidaciones ni injerencias indebidas, y aunque algunos marcos jurídicos pueden otorgar a los fiscales una función de supervisión de la legalidad de las investigaciones[34], dicha supervisión no cumple con los estándares de independencia e imparcialidad que se encuentran en el control judicial. De hecho, como subraya la Comisión Interamericana de Derechos Humanos (CIDH), "las juezas y los jueces son los principales actores para lograr la protección judicial de los derechos humanos en un Estado democrático". Según la CIDH, los jueces son los que garantizan "la convencionalidad, constitucionalidad y legalidad de los actos de otros poderes del Estado y de funcionarios del Estado en general"[35]. Asimismo, el Tribunal Europeo de Derechos Humanos ha afirmado que "el Estado de Derecho implica, *entre otras cosas, que* una injerencia de las autoridades ejecutivas en los derechos de un individuo debe estar sujeta a un control efectivo que normalmente debe ser asegurado por el poder judicial, al menos en última instancia, control judicial que ofrece las mejores garantías de independencia, imparcialidad y un procedimiento adecuado"[36]. Más recientemente, el Tribunal de Justicia de la UE sostuvo que el Ministerio Fiscal, "cuya función es dirigir el procedimiento de instrucción penal y ejercer, en su caso, la acusación pública en un procedimiento posterior", no puede

[34] Directrices de la ONU sobre la función de los fiscales. Adoptadas el 7 de septiembre de 1990 por el Octavo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, párrafo 4 y 11. https://www.ohchr.org/es/instruments-mechanisms/instruments/guidelines-role-prosecutors . Véase también Coalición necesaria y proporcionada sobre normas interamericanas relativas al control judicial de las medidas de vigilancia, https://necessaryandproportionate.org/es/an%C3%A1lisis-jur%C3%ADdico-inter-americano/#vi-autoridad-judicial-competente

[35] Comisión Interamericana de Derechos Humanos. Garantías para la independencia de las y los operadores de justicia. Hacia el fortalecimiento del acceso a la justicia y el estado de derecho en las Américas. OEA/Ser.L./V/II. 5 de diciembre de 2013, párrafo 16. https://www.oas.org/es/cidh/defensores/docs/pdf/operadores-de-justicia-2013.pdf

[36] Véase, en particular, Klass y otros contra Alemania, párrafo 55. https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-57510%22]}. Aunque el Tribunal en el caso Klass estuvo de acuerdo en que "en principio es deseable confiar el control de supervisión a un juez", no llegó a sostener que la autorización judicial previa fuera necesaria en todos los casos, siempre y cuando el organismo de autorización pertinente fuera "suficientemente independiente" de "las autoridades que llevan a cabo la vigilancia" para "emitir un dictamen objetivo" y estuviera también investido "de poderes y competencias suficientes para ejercer un control eficaz y continuo". Sin embargo, en casos posteriores, el Tribunal ha dejado clara la conveniencia de la autorización judicial para el uso de la vigilancia legal. Véase, Kopp v. Suiza, párrafo 74.

considerarse una autoridad administrativa independiente para autorizar el acceso gubernamental a los datos de las comunicaciones en las investigaciones penales[37]. Esto ya se indicó en los *13 Principios sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones*, que reflejan la opinión de que la autorización judicial previa para el acceso gubernamental a los datos no es simplemente deseable, sino esencial[38].

Además, el Informe Explicativo del Protocolo considera que los tipos de información sobre direcciones IP están incluidos en la definición de datos de los abonados del Convenio de Budapest (apartado 3 del artículo 18)[39]. Consciente de que algunos Estados ya conceden un mayor nivel de protección a la divulgación de direcciones IP u otros tipos de números, **el Protocolo permite a las Partes reservarse el derecho a no aplicar este artículo a determinados tipos de números de acceso (artículo 7, apartado 9, letra b)).** Pero esto solo se permite si la revelación de estos números de acceso "sería incompatible con los principios fundamentales de su ordenamiento jurídico interno". Una vez más, una Parte que hace esta reserva no puede dictar requerimientos directos de cooperación para tales números a los proveedores de servicios en los territorios de otras Partes.

Sin embargo, el apartado 9(b) no aborda algunas de las amenazas más problemáticas para la privacidad que plantea el artículo 7, ya que las fuerzas del orden seguirán pudiendo exigir el nombre y la dirección de los abonados a Internet asociados a los números de acceso. El artículo 7 tampoco permite a las Partes optar por no cumplir sus requisitos basándose en otras circunstancias relevantes, como la existencia de inmunidades y privilegios aplicables garantizados en la legislación nacional (por ejemplo, el privilegio abogado-cliente) o los principios básicos de la asistencia mutua internacional. Como se explica más adelante, el artículo 7 disuade de la aplicación sistemática de estos principios al hacer que sus mecanismos de consulta y notificación sean opcionales. Esto supone una amenaza para los derechos humanos, ya que los principios de protección de los derechos consagrados en la legislación nacional o las salvaguardias habituales de las solicitudes de asistencia mutua probablemente no recibirán la consideración adecuada en el marco del procedimiento estándar del artículo 7.

Perú, Paraguay, Argentina, Chile, Brasil, entre muchos otros países de la región, cuentan con protecciones constitucionales o legales tanto respecto al secreto profesional, como al secreto abogado-cliente o médico-paciente y la protección de las fuentes periodísticas[40].

[37] CJUE, Prokuratuur, C-746/18, párrafos 26 y 59.
https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:62018CJ0746&from=en
[38] Coalición necesaria y proporcionada. 13 Principios sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones.
https://necessaryandproportionate.org/global-legal-analysis/#principle-by-principle-explanation
[39] Informe Explicativo del Protocolo, párrafo 93.
[40] En sus comentarios al proyecto de texto del Protocolo, el Consejo de Colegios de Abogados de Europa subrayó que "el secreto profesional/la prerrogativa del abogado puede abarcar no solo los datos de contenido, sino también otros tipos de datos (por ejemplo, datos de tráfico y, en determinadas circunstancias, información relativa a abonados). Además, es necesario ser sensible a las circunstancias en las que se busca la recuperación de los datos de los abonados, que a menudo es el precursor de otras actividades de investigación. Cuando los

Argentina: La Ley 24.767/1997 establece las bases legales para la cooperación internacional en materia penal en Argentina y describe el procedimiento para conceder asistencia cuando no existe un tratado con el Estado requirente. La ley estipula los motivos para denegar una solicitud de asistencia internacional, como por ejemplo: cuando la solicitud se refiere a un delito de derecho penal político o militar; cuando el proceso que motiva la solicitud evidencie propósitos persecutorios por razón de las opiniones políticas, nacionalidad, raza o religión o cuando existen motivos para suponer que esas razones pueden perjudicar el derecho de defensa de una persona, y cuando el delito en cuestión está castigado con la pena de muerte en el Estado que solicita la asistencia y no se ofrece seguridades de que esa pena no será aplicable[41].

De acuerdo con el procedimiento estándar del artículo 7, corresponde al proveedor de servicios evaluar si las autoridades extranjeras del Estado Parte que dictan los requerimientos de datos son legítimas, si la orden es legal y proporcionada o si pone en peligro los derechos humanos de los interesados, o si se aplica algún motivo de denegación. Si no verifican la legislación vigente en el lugar donde se encuentran y no tienen un conocimiento razonable del contexto extranjero en el que se emitió el requerimiento directo, los proveedores de servicios corren el riesgo de revelar datos de una forma no autorizada por la legislación nacional. La autoridad que emite el requerimiento de datos no está obligada a proporcionar un resumen de los hechos relacionados con la investigación o el procedimiento, que podría arrojar luz sobre circunstancias incompatibles con los derechos humanos. Las autoridades de la Parte en la que se encuentra el proveedor de servicios, que tienen la facultad de recibir y solicitar información adicional sobre los hechos, están, por defecto, excluidas de los requerimientos directos de cooperación en virtud del artículo 7.

Aunque las grandes empresas tecnológicas pueden estar mejor equipadas para gestionar requerimientos directos del extranjero, también se enfrentarán a dificultades para identificar y rechazar los requerimientos transfronterizos de datos de los abonados que sean contrarios a los derechos humanos. Mientras tanto, las empresas de telecomunicaciones locales o los proveedores de servicios más pequeños tienen una capacidad y una experiencia significativamente menores para gestionar este tipo de pedidos, lo que será aún más perjudicial para los derechos humanos.

---

datos se refieran a abogados, su recuperación conllevará un riesgo considerable de violación posterior del secreto profesional de los abogados en sus comunicaciones con sus clientes, e incluso cuando los datos de los abonados se refieran a personas que no sean abogados, puede existir el riesgo de que la investigación posterior dé lugar a una violación de las comunicaciones privilegiadas".
https://rm.coe.int/ccbe-written-comments-draft-2nd-additional-protocol-to-the-convention-/168098bc6e

[41] Véase el artículo 67 combinado con el artículo 8 de la Ley 24.767/1997.
http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/41442/norma.htm

Los requerimientos transfronterizos directos pueden plantear muchos problemas prácticos a los proveedores de servicios. Además de carecer de los conocimientos y/o la información necesarios para revisar la legalidad, la proporcionalidad y el contexto local de dichas solicitudes, estos retos implican la ausencia de canales de contacto establecidos o conocidos con las autoridades extranjeras requirentes. La verificación de la autenticidad de un requerimiento y la garantía de mecanismos seguros para la transmisión de datos no son sencillas[42] e incluso las grandes empresas pueden cometer graves errores[43]. El artículo 7, apartado 6, establece únicamente que "*podrán* exigirse niveles adecuados de seguridad y autenticación" en caso de que los datos se faciliten en formato electrónico. El Informe Explicativo indica que el uso de una dirección de correo electrónico oficial podría ser suficiente para afirmar la autenticidad de una solicitud, lo que no deja de ser fácil de manipular[44]. Obtener la confirmación de la autenticidad a través de una autoridad conocida en la Parte requirente, otro método sugerido, puede ser mejor pero más complejo para los proveedores más pequeños que no están acostumbrados a gestionar los requerimientos de las autoridades extranjeras.

Todo ello refuerza la importancia de que una autoridad de la Parte en la que se encuentra el proveedor de servicios participe en la tramitación de dichas solicitudes. Como salvaguardias opcionales, **el artículo 7 del Protocolo permite a una Parte exigir que sus autoridades reciban una *notificación* simultánea cuando se emita un requerimiento directo de cooperación y/o ordenar a los proveedores de servicios que *consulten* a las autoridades de la Parte antes de la divulgación ((artículo 7, párrafo 5 (a) y (b)).** Entre ambas posibilidades, la exigencia de notificación simultánea es la más adecuada para la protección de los derechos humanos. Según el artículo 7, apartado 5, letra c), las autoridades notificadas o consultadas podrán ordenar al proveedor de servicios que no revele la información del abonado si (i) la revelación puede ir en detrimento de investigaciones o procesos en el territorio de esa Parte; o (ii) se aplicarían condiciones o motivos de denegación si la información relativa a abonados se hubiera solicitado mediante asistencia mutua en virtud del Convenio de Budapest. Las autoridades notificadas o consultadas también pueden obtener información adicional que no se compartiría con el proveedor de servicios (artículo 7, párrafo 5(c)(i)). En cualquier caso, el Informe Explicativo del Protocolo señala que los impedimentos a la cooperación y las denegaciones de solicitudes deben ser "estrictamente limitados"[45].

El artículo 7, párrafo 5(e), estipula además que las Partes deben designar una sola autoridad para recibir la notificación y/o la consulta y realizar las actuaciones relacionadas. Esta es una oportunidad clave para que los Estados Parte asignen una autoridad judicial independiente para cumplir estas funciones y revisar los requerimientos directos transfronterizos. En el contexto de la Unión Europea, el

[42] EuroISPA abordó estos y otros problemas prácticos en sus comentarios al proyecto de texto del Protocolo. Véanse, por ejemplo, las presentaciones de EuroISPA a las rondas de consulta 4ª y 6ª (nota 18 supra).
[43] Según los medios de comunicación, Apple y Meta proporcionaron detalles de los usuarios, como la dirección del cliente, el número de teléfono y la dirección IP, en respuesta a falsas "solicitudes de datos de emergencia" realizadas por los "hackers". Véase en: https://www.bloomberg.com/news/articles/2022-03-30/apple-meta-gave-user-data-to-hackers-who-forged-legal-requests
[44] Informe Explicativo del Protocolo, párrafo 116.
[45] Informe explicativo del Protocolo, párrafos 108-110.

Supervisor Europeo de Protección de Datos (SEPD) recomendó dar instrucciones a los Estados miembros para que designen una autoridad judicial u otra autoridad independiente para recibir la notificación. El SEPD también destacó la importancia de una participación sistemática de las autoridades judiciales en las Partes requeridas para preservar el principio de doble incriminación[46].

En resumen, según el procedimiento por defecto del artículo 7, *cualquier* autoridad competente[47] de la Parte requirente, sujeta a su propia legislación nacional, puede emitir un requerimiento directo a un proveedor de servicios situado en el territorio de otra Parte para acceder a los datos de los abonados, basándose en una definición amplia de la información relativa a abonados. Ninguna autoridad nacional interviene en el análisis y la tramitación de esta orden en la Parte requerida, y mucho menos una autoridad judicial u otra independiente. Con esto, en ciertos casos, los proveedores de servicios pueden tener que revelar la información relativa a abonados a los Estados extranjeros bajo un estándar inferior a la que están sujetos cuando responden a las solicitudes de las autoridades nacionales.

Si bien es cierto que las investigaciones o procedimientos por delitos de naturaleza totalmente interna[48] pueden requerir a veces que las autoridades policiales busquen datos en el extranjero, la aplicación del artículo 7 no limita los requerimientos directos transfronterizos a esos casos internos, en los que podría parecer que la Parte requerida no tiene intereses en juego. El artículo 7 también se aplica a los casos en los que están implicadas personas que se encuentran o viven en la Parte requerida. E, incluso en los casos totalmente internos del Estado requirente, la Parte requerida puede considerar fundamental denegar las solicitudes de asistencia en apoyo de investigaciones o procesos que estén motivados por razones políticas o discriminatorias, que infrinjan la libertad de expresión o la constitución del país, que estén relacionados con un delito político o que impliquen un delito castigado con la pena de muerte. Se trata de salvaguardias que pueden encontrarse en determinados acuerdos de asistencia jurídica mutua y normas conexas[49].

---

[46] La Comisión Europea adoptó dos propuestas para que el Consejo Europeo decida si autoriza a los Estados miembros a firmar y ratificar el Protocolo en interés de la UE. En su Dictamen 1/2022, el SEPD acoge con satisfacción las propuestas de la Comisión para que los Estados miembros hagan la declaración prevista en el artículo 7(5)(a) del Protocolo, para exigir la notificación simultánea de los requerimientos directos de cooperación, y recomienda además que la autoridad designada sea una autoridad judicial u otra autoridad independiente. Véanse los párrafos 90-92 en https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-two-proposals-council-decisions_en

[47] Véase la nota 12 supra para la definición de "autoridades competentes" del Protocolo.

[48] Situaciones en las que el delito, la víctima y el autor se encuentran en el mismo país que la autoridad investigadora.

[49] Véase el ejemplo de la Ley 24.767/1997 de Argentina. Para otros ejemplos, véase: Convenio Europeo de Asistencia Judicial en Materia Penal, artículo 2, https://rm.coe.int/16800656ce. MLAT Brasil e Itália, Artículo 3, http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0862.htm. MLAT Brasil y Perú, artículo 3, http://www.planalto.gov.br/ccivil_03/decreto/2001/D3988.htm. MLAT EE.UU. y Kazajstán (análisis del artículo 3), https://www.congress.gov/114/cdoc/tdoc11/CDOC-114tdoc11.pdf. El MLAT de EE.UU. con Bermudas establece que un "requerimiento también puede ser denegado si se relaciona con un delito político o militar, si no se ajusta a los requisitos del Tratado, o si su ejecución perjudicaría la soberanía, la seguridad u otros intereses esenciales de la Parte requerida, o sería contraria a una política pública importante. Con respecto a este último motivo, el gobierno de Bermuda indicó que tiene la intención de interpretar la disposición para

Es más, las asimetrías y los supuestos fomentados en la justificación del artículo 7 pueden servir de influencia sistemática para rebajar las normas de protección alcanzadas por los Estados Parte a nivel nacional, tal y como analizamos en la siguiente sección.

En general, las preocupaciones descritas en esta guía se refieren no solo a las amenazas a los derechos humanos en el contexto del acceso transfronterizo a los datos, sino que probablemente afectarán a los marcos nacionales de privacidad relacionados con las investigaciones penales en los países latinoamericanos.

¿Cómo puede el artículo 7 afectar negativamente a los marcos de privacidad latinoamericanos?

El artículo 7 puede afectar negativamente a los marcos legales privacidad de las comunicaciones de América Latina de varias maneras:

- Puede desempeñar un papel influyente en el establecimiento de un nivel de protección inferior para acceder a los datos de los abonados y desvelar la identidad de un usuario. El Protocolo se basa en la distinción del Convenio de Budapest entre los datos relativos a abonados y otros datos de las comunicaciones para establecer un nivel de protección más bajo para el acceso transfronterizo a la información de los abonados, basándose en la suposición errónea, reflejada en el Informe Explicativo del Protocolo, de que este tipo de datos "no permite sacar conclusiones precisas sobre la vida privada y los hábitos diarios de las personas afectadas". Tanto la distinción como la suposición pasan por alto que los datos relativos a abonados son muy codiciados para las investigaciones penales porque, cuando se combinan con datos de contenido o de tráfico que ya están en posesión del Estado o que pueden obtenerse, vincularse o referenciarse fácilmente, pueden utilizarse para identificar a personas concretas implicadas en actividades expresivas, su ubicación y otras informaciones sensibles;
- Con el paso del tiempo, el TC-Y ha emitido directrices que pretenden interpretar ampliamente la definición de información relativa a abonados del Convenio de Budapest para incluir las direcciones IP—entendimiento que también puede desempeñar un papel influyente en los marcos de la región;
- El artículo 7 también obstaculiza el compromiso de las empresas con las mejores prácticas para interpretar las leyes locales de manera que proporcionen una sólida protección de la privacidad de los usuarios (e.j., exigir una orden judicial para entregar la información de los suscriptores a las autoridades policiales), lo que vemos en países como Chile (véase el cuadro 1);
- Por último, no establece garantías de privacidad obligatorias para los Estados Parte. El artículo 7 establece claras facultades transfronterizas de obtención de pruebas al más alto nivel para acceder a los datos relativos a abonados, pero no

otorgar a Bermuda el derecho a negar la asistencia en casos que impliquen la pena capital".
https://www.congress.gov/111/cdoc/tdoc6/CDOC-111tdoc6.pdf.

> establece una protección mínima obligatoria de base para cuando las autoridades puedan acceder a los datos de los abonados. Según el procedimiento estándar del artículo 7, las salvaguardias aplicadas a los requerimientos transfronterizos directos a los proveedores de servicios se basan en el marco nacional de la Parte que solicita los datos, y no en las garantizadas en el territorio donde se encuentra el proveedor de servicios requerido.

Un reciente análisis de las tendencias de la cooperación internacional para acceder a las pruebas digitales realizado por la Dirección Ejecutiva del Comité contra el Terrorismo (CTED) del Consejo de Seguridad de la ONU señala:

> "[...] si los Estados aceptan normas más bajas para las investigaciones transfronterizas que las que aplican en su país, puede haber presiones para rebajar la norma en el país (ya que sería extraño que fuera más fácil para los investigadores extranjeros que para los nacionales acceder a las pruebas digitales en un determinado Estado)"[50].

El artículo 7 se alinea con las normas de privacidad de las comunicaciones más débiles de América Latina[51]. En las disputas nacionales relativas a las garantías de privacidad para el acceso a los datos relativos a abonados, las influyentes normas del CdE y las concepciones subyacentes pueden utilizarse para inclinar la balanza en contra de las protecciones fuertes. Por ejemplo, reformas legislativas tanto en Chile[52] como en Brasil[53] han propuesto permitir el acceso de la policía a los datos de los abonados sin autorización judicial previa, buscando terminar con las interpretaciones más protectoras de la legislación aplicable actual.

Mientras que los tribunales nacionales de todo el mundo, incluidos los de América Latina [54], reconocen cada vez más que los datos relativos a abonados pueden revelar

[50] Dirección Ejecutiva del Comité contra el Terrorismo del Consejo de Seguridad de las Naciones Unidas. The State Of International Cooperation For Lawful Access To Digital Evidence: Research Perspectives: Privacy & Human Rights in CrossBorder Law Enforcement https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Jan/cted_trends_report_lawful_access_to_digital_data_.pdf

[51] Véase Katitza Rogriguez, Veridiana Alimonti. Cuando las fuerzas del orden quieren sus comunicaciones privadas, ¿Qué garantías legales existen en América Latina y España si las fuerzas del orden quieren tus comunicaciones privadas? 2 de febrero de 2021. https://www.eff.org/es/deeplinks/2021/02/when-law-enforcement-wants-your-private-communications-what-legal-safeguards-are. Véase también A pesar del progreso, los metadatos aún tienen una protección de "segunda clase" en Latam. 3 de febrero de 2021. https://www.eff.org/es/deeplinks/2021/02/despite-progress-metadata-still-under-second-class-protection-latam-legal

[52] Ver Michelle Bordachar. Nueva ley de delitos informáticos. 20 de diciembre de 2021. https://www.derechosdigitales.org/17457/nueva-ley-de-delitos-informaticos/

[53] Véase más información sobre las disputas en torno a las salvaguardias aplicadas al acceso de las fuerzas de seguridad a los datos de los abonados en Brasil en Veridiana Alimonti y Karen Gullo. De no haber cambios, el proyecto de Tratado de Vigilancia Policial del Consejo de Europa será una influencia perniciosa en los marcos legales de privacidad de Latinoamérica. 3 de septiembre de 2021. https://www.eff.org/es/deeplinks/2021/09/without-changes-council-europes-draft-police-surveillance-treaty-pernicious

[54] En una sentencia histórica que afirma la protección de datos como un derecho fundamental en la Constitución de Brasil, los jueces del Tribunal Supremo del país señalaron cómo los cambios en nuestro

información crítica sobre la vida de las personas, el Protocolo no solo fomenta la visión contraria, sino que en gran medida congela una norma más débil para la revelación transfronteriza de la información de los abonados, ya que las reservas al artículo 7 solo se permiten en el momento en que el Estado se adhiere al Protocolo.

Si los ordenamientos jurídicos nacionales, debido a nuevas leyes o decisiones judiciales, reconocen finalmente salvaguardias adicionales para la información relativa a abonados después de ratificar el Protocolo, como la necesidad de autorización judicial previa, el Estado no podrá invocar las reservas del apartado 9 del artículo 7 para bloquear los requerimientos directos de cooperación o impedir que se utilicen para revelar ciertos tipos de números de acceso (por ejemplo, las direcciones IP de inicio de sesión). Además, los Estados Parte solo pueden excluir la divulgación de ciertos tipos de números de acceso en virtud del artículo 7 cuando hacer lo contrario "sería incompatible con los principios fundamentales de [el] ordenamiento jurídico interno". Mientras que la legislación brasileña, por ejemplo, exige expresamente una orden judicial antes de la revelación de las direcciones IP, en muchos sistemas jurídicos latinoamericanos, el control judicial y/o la necesidad de motivos razonables para acceder a los datos de las comunicaciones no están claramente explicitados en la ley. Dichas salvaguardias a menudo se basan en legislación que no distingue explícitamente los tipos de información o se basan en jurisprudencia que aborda las protecciones en el contexto de las comunicaciones telefónicas[55].

En el mismo sentido, hacer una declaración para exigir la supervisión fiscal y judicial de los requerimientos directos extranjeros solamente se permite a las Partes cuando firman o ratifican el Protocolo (en virtud del artículo 7.2.b)). La inclusión obligatoria de "fiscales" en la declaración permitida impide a los signatarios exigir a la Parte requirente que someta sus requerimientos directos únicamente a supervisión judicial. Sin embargo, el Estado requerido puede garantizar el control judicial de los requerimientos directos transfronterizos recibidos en su territorio exigiendo que se les notifiquen simultáneamente a las autoridades judiciales locales (artículo 7, apartado 5, letras a) y e)). El Protocolo no estipula un plazo final para que las Partes lo invoquen.

panorama tecnológico exigen un tratamiento más cauteloso de la información de los abonados. Recordaron las guías telefónicas públicas que contenían los nombres, los números de teléfono y las direcciones de las personas, afirmando que "lo que se podía hacer a partir de la publicación de esos datos personales [hace unas décadas] no es comparable a lo que se puede hacer en el nivel tecnológico actual, en el que potentes tecnologías de tratamiento de datos, cruce y filtrado permiten la formación de perfiles individuales extremadamente detallados". https://jurisprudencia.stf.jus.br/pages/search/sjur436273/false

[55] Véase, por ejemplo, la decisión de la Corte Suprema de Argentina en el caso Halabi. http://www.saij.gob.ar/corte-suprema-justicia-nacion-federal-ciudad-autonoma-buenos-aires-halabi-ernesto-pen-ley-25783-dto-1563-04-amparo-ley-16986-fa09000006-2009-02-24/123456789-600-0009-0ots-eupmocsollaf

(b) Desequilibrio entre las salvaguardias y los poderes de aplicación de la ley en el Protocolo

Las facultades de aplicación de la ley que establece el Protocolo son en su mayoría obligatorias para todos los signatarios, mientras que muchas de sus salvaguardias en materia de derechos humanos no son esenciales o son aplicables en función de las normas generales derivadas de los marcos jurídicos nacionales y de las obligaciones de los Estados en materia de derechos humanos.

El artículo 7 refleja este desequilibrio. Como se ha visto en la sección anterior, la mayoría de sus salvaguardias son opcionales y dependen de las reservas y declaraciones de los Estados Parte. Otras disposiciones también contienen declaraciones opcionales que pueden ser invocadas por las Partes y que merecen atención dentro de los debates nacionales sobre la adhesión al Protocolo. Por ejemplo, otra declaración relevante se encuentra en el párrafo 4 del artículo 8, por el que las Partes pueden declarar que se requiere información de apoyo adicional para dar efecto a los requerimientos para la presentación rápida de información relativa a abonados y datos relativos al tráfico. La información pertinente puede variar en cada caso, por lo que los Estados pueden declarar que la información de apoyo adicional requerida dependerá de las circunstancias del requerimiento y de la investigación o el procedimiento relacionado. **Una lista resumida puede encontrarse en el artículo 19, que señala todas las reservas y declaraciones presentes en las disposiciones del Protocolo.**

Esta sección se centra en el Capítulo III del Protocolo. Establece las salvaguardias de los derechos humanos y de la privacidad que se aplican cuando los Estados se apoyan en los poderes señalados por el Protocolo.

Condiciones y garantías del artículo 13

El artículo 13 reconoce la obligación general de garantizar una protección adecuada de los derechos humanos y las libertades fundamentales. Se basa en las salvaguardias generales del Convenio de Budapest para estipular que el establecimiento y la aplicación de los poderes y procedimientos del Protocolo están sujetos a las condiciones y salvaguardias del derecho interno de los Estados. Esto es especialmente importante en lo que respecta a la obligación de incorporar el principio de proporcionalidad al determinar el alcance de las salvaguardias de los derechos humanos. Sin embargo, se deja que las Partes determinen en gran medida qué protecciones son "adecuadas" y "proporcionadas" sobre la base de la legislación nacional. Varios países de la región se basan en el principio de proporcionalidad a la hora de equilibrar y restringir los derechos

fundamentales en la jurisprudencia[56] y en las normas procesales penales[57]. Sin embargo, la interpretación y la aplicación del principio varían ampliamente en los distintos marcos nacionales y, en la práctica, el artículo 13 impone pocas obligaciones directas a los Estados Parte para que impongan garantías específicas en contextos de investigación concretos.

Sin embargo, debemos tener en cuenta que las salvaguardias aplicables incluyen los derechos derivados de las obligaciones asumidas por los Estados en virtud de acuerdos internacionales de derechos humanos. El artículo 17 del Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas y el artículo 11 de la Convención Americana sobre Derechos Humanos son los referentes universales y regionales entre los Estados latinoamericanos para los derechos y salvaguardias aplicables según el artículo 13 del Protocolo[58].

Salvaguardias de protección de datos del artículo 14

El artículo 14 estipula una serie de obligaciones detalladas de protección de datos aplicables a cualquier información personal obtenida a través de las facultades policiales del Protocolo. Esto tiene especial importancia en América Latina, ya que muchas leyes de protección de datos de la región excluyen de su ámbito de aplicación las investigaciones y los procedimientos penales, y no existen otras normas de protección de datos específicas para las actividades policiales, como ocurre en la UE con la Directiva 2016/680 (*Law Enforcement Directive*).

No obstante, el artículo 14 presenta deficiencias preocupantes con respecto a otras normas internacionales, en particular el propio Convenio 108/108+ del Consejo de Europa (Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y su protocolo de modificación). En América Latina, Argentina, México y Uruguay son Partes del Convenio 108 de 1981. Hasta ahora, Argentina ha firmado y Uruguay ha ratificado el protocolo de modificación del Convenio 108 (Convenio 108+)[59]. Además, las salvaguardias del artículo 14 pueden ser eludidas por los signatarios del Protocolo. A continuación exponemos estas preocupaciones.

---

[56] Por ejemplo, existe una rica jurisprudencia sobre el principio de proporcionalidad en Argentina (como las decisiones 248:800; 243:449; 334:516; 335:452; 313:1638; 330:855; y 334:516) y en Chile (https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-52002012000100003). En Perú, el primer y más referenciado precedente se encuentra bajo el caso n. 045-2004-PI/TC, disponible en https://www.tc.gob.pe/jurisprudencia/2006/00045-2004-AI.pdf

[57] Podemos mencionar como ejemplos el artículo VI del Título Preliminar y el artículo 203 del Código Procesal Penal de Perú, el artículo 276 del Código Procesal Penal de Chile y, entre otros, el artículo 12 del Código Procesal Penal de Panamá.

[58] Es importante señalar que los poderes de recopilación de pruebas del Protocolo no se limitan a la información de registro de nombres de dominio (artículo 6), a la información relativa a abonados (artículos 7 y 8) y a datos relativos al tráfico (artículo 8). Estos poderes también incluyen la revelación del contenido de las comunicaciones, por ejemplo, a través del artículo 9, que aborda la revelación rápida de datos informáticos almacenados en caso de emergencia.

[59] Véanse las firmas y ratificaciones del Convenio 108+ en https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223. El Protocolo de Enmienda entrará en vigor una vez que todas las Partes del Convenio 108 de 1981 hayan ratificado el acuerdo o el 11 de octubre de 2023 si en esa fecha hay 38 Partes del Convenio 108+.

1. Debilitamiento de las competencias relacionadas con la evaluación de un nivel adecuado de protección en las transferencias internacionales de datos personales

Una serie de leyes de protección de datos facultan a las autoridades nacionales de supervisión para evaluar si los países terceros proporcionan un nivel de protección equivalente[60]. Con ello, pretenden garantizar que los derechos de las personas puedan fluir junto con sus datos en las transferencias internacionales de datos. Algunas de estas leyes también facultan a las autoridades a suspender las transferencias de datos personales cuando no se cumple dicho nivel de protección. Del mismo modo, el protocolo de modificación del Convenio 108 del Consejo de Europa estipula que las transferencias internacionales a destinatarios bajo la jurisdicción de Estados que no sean Partes del Convenio 108/108+ solo podrán realizarse cuando se garantice un nivel adecuado de protección basado en sus disposiciones. También establece que los firmantes deberán facultar a sus autoridades de protección de datos para que tomen medidas para salvaguardar los derechos de los interesados en las transferencias internacionales de datos. Estas medidas incluyen exigir a las entidades que demuestren que las salvaguardias existentes son eficaces, que prohíban o suspendan las transferencias, o que sometan las transferencias a condiciones que protejan los derechos y las libertades del interesado[61]. Sin embargo, como explicamos a continuación, el Protocolo limita estas facultades de aplicación de la protección de datos en los Estados Parte en los que ellas serían aplicables:

1.a. Evaluación de un nivel de protección equivalente para las transferencias de datos personales a terceros países: Según la letra d) del apartado 1 del artículo 14, cada Parte considerará que el tratamiento de datos personales en virtud de los apartados 2 a 15 del artículo 14 del Protocolo, o en virtud de acuerdos previos de transferencia internacional de datos entre las Partes, cumple los requisitos de los marcos jurídicos de protección de datos de las Partes para las transferencias internacionales de datos personales. Con ello, y dado que las protecciones pertinentes establecidas en los apartados 2 a 15 dependen de cómo se articulen en las legislaciones nacionales de los Estados[62], el Protocolo pide a las Partes que asuman un nivel de protección que puede ser significativamente débil en los marcos nacionales de otras Partes[63]. Lamentablemente, el Protocolo no ha garantizado la capacidad de las Partes para evaluar el nivel de protección de la Parte requirente antes de permitir las transferencias[64].

[60] En el contexto de los Estados miembros de la UE, la autoridad encargada de esta evaluación es la Comisión Europea.
[61] Véase el artículo 14, apartado 6, del Convenio 108+.
https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000016807c65bf
[62] Véase, por ejemplo, el artículo 14, apartado 2(a), apartado 5, apartado 11(b) y apartado 12(a).
[63] La organización de derechos digitales Access Now planteó esta preocupación en su presentación a la sexta ronda de consultas del proyecto de texto del Protocolo. https://rm.coe.int/0900001680a25783
[64] En la mencionada presentación, Access Now recomendó a los redactores del Protocolo que sustituyeran el apartado 1(d) del artículo 14 por "un requisito de que cada Parte evalúe, con la autoridad de supervisión pertinente para la protección de datos, el nivel de protección de la Parte requirente antes de permitir las transferencias". El Comité T-CY no siguió la recomendación.

1.b. Suspensión de las transferencias internacionales de datos: Aunque el Protocolo permite a las Partes suspender las transferencias de datos si se infringen las salvaguardias del artículo 14, esto solo es posible con "pruebas sustanciales" de una "infracción sistemática o sustancial" o de que una "infracción sustancial es inminente", y después de entablar consultas con el Estado suspendido (artículo 14, apartado 15)[65]. Esto pone un listón muy alto en comparación con otros instrumentos, como el RGPD y el Convenio 108/108+[66]. Además, el Protocolo no prevé un mecanismo de cooperación entre las autoridades de protección de datos a través del cual podría realizarse dicha consulta. En el contexto de un acuerdo internacional, esta consulta tendrá lugar a nivel gubernamental. Las autoridades de protección de datos facultadas por la ley para suspender las transferencias tendrán que implicar y obtener el acuerdo de su gobierno nacional. Esto socava la independencia de las autoridades de supervisión de la protección de datos en las Partes en las que dicha independencia está garantizada[67].

2. Confidencialidad de las transferencias de datos frente a los derechos de información y acceso de los interesados

El Protocolo no exige a los signatarios que proporcionen notificaciones personales a las personas afectadas por las transferencias transfronterizas de datos basadas en las competencias del Protocolo. Según el artículo 14, párrafo 11(a), los Estados solamente pueden proporcionar avisos generales al público (por ejemplo, en un sitio web gubernamental)[68]. No está claro cómo las personas afectadas podrían entender que una solicitud de datos revelada se refiere a su información personal, y en cierto modo se asume que las personas consultan regularmente los sitios web o los repositorios que muestran tales avisos generales. Con esta suposición, el Protocolo termina por aceptar una notificación ineficaz como medida suficiente. Sin una notificación individual (ya sea del proveedor de servicios o de las autoridades del Estado requirente o del Estado requerido) las personas no tendrán ninguna forma real o efectiva de saber que sus datos personales han sido transferidos a las autoridades policiales de otro país. Esto hace caso omiso de los estándares internacionales que reconocen la importancia de la notificación individual para garantizar los derechos de recurso y un tratamiento justo de los datos personales de las personas afectadas[69]. Además, incluso cuando la notificación es

[65] Excepcionalmente, una Parte puede suspender las transferencias antes de iniciar la consulta. De acuerdo con el artículo 14, párrafo 15, una Parte podrá suspender provisionalmente las transferencias en caso de infracción sistemática o sustancial que plantee un riesgo significativo e inminente para la vida o la seguridad de una persona física, o un perjuicio sustancial para su reputación o su patrimonio, en cuyo caso lo notificarán a la otra Parte y la consultarán inmediatamente después.

[66] Véanse el artículo 46 y el apartado 2 del artículo 58 del RGPD y los apartados 2 a 6 del artículo 14 del Convenio 108+.

[67] Conforme EDRi (European Digital Rights) señala en su paper Ratification by EU Member States of the Second Additional Protocol of the Council of Europe Cybercrime Convention, 2022, p. 7. https://edri.org/wp-content/uploads/2022/04/EDRi-Position-Ratification-EU-Member-States-Cybercrime-Second-Additional-Protocol.pdf

[68] Véase el Informe Explicativo del Protocolo, párrafo 267.

[69] El Relator Especial de las Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y de expresión ha subrayado que "[l]as personas deben tener derecho a que se les notifique si han estado sometidas a la vigilancia de las comunicaciones o si el Estado ha accedido a sus datos de comunicaciones. Si bien la notificación por adelantado o simultánea podría atentar contra la eficacia de la

obligatoria en la Parte requerida, el Protocolo permite a la Parte que requiere los datos restringir, en las condiciones establecidas en su propio derecho interno, cualquier requisito de notificación personal que pueda existir en el derecho nacional de la Parte requerida, siempre que las restricciones sean necesarias para proteger los derechos y libertades de terceros u objetivos importantes de interés público general y que tengan debidamente en cuenta los intereses legítimos de la persona afectada. "Objetivos importantes de interés público general" es una cláusula amplia que puede abarcar mucho más que la protección de las investigaciones en curso para que no se vean comprometidas. Además, el artículo 14 no exige una supervisión independiente de las transferencias secretas de datos y no establece ningún plazo para poner fin a las restricciones de confidencialidad. Los países con obligaciones de notificación establecidas como salvaguardia en la legislación nacional probablemente se verán obstaculizados a la hora de aplicar esas leyes en contextos transfronterizos.

Las mismas limitaciones se aplican al derecho de los interesados a acceder a los datos personales (artículo 14, apartado 12(a)(i)), que los signatarios deben garantizar de acuerdo con su marco jurídico nacional. Como ha señalado el Supervisor Europeo de Protección de Datos, aunque el Protocolo establece positivamente normas para calibrar las restricciones al derecho de acceso, no garantiza que los interesados puedan, *de hecho*, ejercer este derecho[70].

3. Datos biométricos

El enfoque del Protocolo respecto a los datos biométricos socava el creciente entendimiento internacional de que este tipo de datos es sensible y requiere una protección adicional dada su capacidad para identificar persistentemente a las personas a través de medios automatizados. Los datos biométricos implican representaciones matemáticas de los rasgos personales de las personas, como sus huellas dactilares, de voz o del iris, y alimentan una serie de tecnologías intrusivas como el reconocimiento facial. El artículo 14, párrafo 4, considera que los datos biométricos son sensibles solo "en vista de los riesgos que entrañan"[71]. El Protocolo ofrece poca orientación sobre lo que podría constituir este riesgo añadido, reduciendo el alcance de la protección de los datos biométricos en comparación con leyes competidoras como el RGPD, la Directiva (UE) 2016/680, el Convenio 108+ del Consejo de Europa y las normativas de protección

vigilancia, debe notificarse a las personas una vez que la vigilancia haya finalizado, y darles posibilidad de obtener reparación por el uso de medidas de vigilancia, con posteridad a ella". UN Doc A/HRC/23/40. 17 de abril de 2013, párrafo. 82. Disponible en https://undocs.org/A/HRC/23/40. Véase también el Dictamen 1/15 del Tribunal de Justicia de la UE sobre el Acuerdo PNR UE-Canadá, ECLI:EU:C:2017:592, párrafo. 220. https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:62015CC0001&from=en

[70] Supervisor Europeo de Protección de Datos. Dictamen 1/2022 (véase la nota 46 supra), párrafos 99 y 107. "[el SEPD] lamenta, sin embargo, que el Protocolo no exija que el marco jurídico nacional de las Partes se asegure de que la posibilidad de que los interesados tengan acceso a sus propios datos, de facto, exista, aunque sea limitada o se ejerza a través de una autoridad".

[71] Informe Explicativo del Protocolo, párrafo 237. "Dado que el nivel de sensibilidad de los datos biométricos puede variar, el párrafo 4 proporciona flexibilidad a las Partes para regular este ámbito indicando que los datos sensibles incluyen "los datos biométricos considerados sensibles en vista de los riesgos que conllevan". Esta redacción reconoce que la biometría es un campo en evolución y que los datos que se consideran "sensibles" en virtud de este párrafo deberán evaluarse con el tiempo en conjunción con los avances tecnológicos, de investigación y de otro tipo, así como con los riesgos para la persona implicada."

de datos de los países latinoamericanos. Todas ellas reconocen la sensibilidad de los datos biométricos cuando se utilizan para identificar de forma exclusiva a las personas, independientemente de los riesgos que conllevan[72].

Colombia, Brasil y Panamá son ejemplos de países latinoamericanos con leyes de protección de datos que incluyen, sin más condiciones, los datos biométricos en la definición de datos personales sensibles.

4. Vías para eludir las garantías de protección de datos del Protocolo

En virtud del artículo 14, párrafo 1, se permite explícitamente a los signatarios eludir las salvaguardias de protección de datos detalladas en los párrafos 2 a 15 mediante otros acuerdos internacionales. En contraste con los poderes de aplicación de la ley establecidos en el Protocolo, se permite a las Partes determinar mutuamente que las transferencias de datos personales bajo su poder pueden producirse según los términos elaborados en acuerdos o arreglos sustitutivos que se aplicarán "en lugar de los apartados 2 a 15" (Artículo 14, párrafo 1(c)). No existe la obligación de garantizar que los acuerdos sustitutivos protejan adecuadamente los datos o empleen salvaguardias comparables a las establecidas en el artículo 14. Tampoco se exige que dichos acuerdos o arreglos se hagan públicos[73].

Resulta especialmente preocupante cómo la combinación de los artículos 12 y 14 puede afectar a la protección de datos en determinadas jurisdicciones. Mientras que este último permite a las Partes eludir sus salvaguardias de protección de datos por acuerdo mutuo, el artículo 12 faculta a las autoridades policiales de primera línea a celebrar acuerdos informales para regir investigaciones conjuntas específicas sobre una base ad hoc en nombre de los signatarios del Protocolo. La supervisión de la conducta investigadora transfronteriza en el marco de estos equipos conjuntos se deja en gran medida en manos de las fuerzas policiales locales. El impacto combinado de estas dos disposiciones parece ser que los funcionarios de primera línea pueden eludir las salvaguardias de protección de datos del Protocolo, sin ninguna aprobación o aportación de las autoridades gubernamentales de las otras Partes y sin transparencia sobre lo que se ha acordado. Además, el artículo 12, párrafo 5, autoriza a los organismos encargados de la aplicación de la ley a eludir los acuerdos de asistencia mutua formalizados ya en vigor para tareas de investigación específicas. A pesar de la recomendación de las organizaciones de la sociedad civil de enmendar el proyecto de texto del Protocolo para evitar que los acuerdos de los equipos conjuntos de investigación sustituyan las salvaguardias de

[72] Véanse el apartado 14 del artículo 4 y el apartado 1 del artículo 9 del RGPD, el apartado 13 del artículo 3 y el artículo 10 de la Directiva (UE) 2016/680, y el apartado 1 del artículo 6 del Convenio 108+.
[73] Véase el Informe Explicativo del Protocolo, párrafo 223. "Con el fin de proporcionar seguridad jurídica y transparencia a las personas y a los proveedores y entidades que participan en las transferencias de datos de conformidad con las medidas de la sección 2 del capítulo 2 del presente Protocolo, se alienta a las Partes a comunicar claramente al público su determinación mutua de que dicho acuerdo o arreglo rige los aspectos de protección de datos de las transferencias de datos personales entre ellas." [el subrayado es nuestro].

protección de datos del Protocolo[74], el texto adoptado no excluye claramente esta posibilidad.

Al menos una parte de estos problemas puede mitigarse mediante la declaración permitida en el **artículo 12, párrafo 3, por la que las Partes pueden exigir que su autoridad central sea signataria del acuerdo por el que se cree el equipo, o intervenir de otro modo en este acuerdo.** Los países que se adhieran al Protocolo deberían considerar seriamente la posibilidad de invocar dicha cláusula. Una vez más, esto solo se permite en el momento de la firma o al depositar su instrumento de ratificación, aceptación o aprobación.

[74] Véase EFF, Derechos Digitales, EDRi, Fundación Karisma, CIPPIC y TEDIC. Privacy & Human Rights in Cross-Border Law Enforcement, (nota 17 supra), p. 13. Véanse otras cuestiones relativas a la regulación de los equipos conjuntos de investigación en el marco del Protocolo en la sección 2 de este documento.

III. Evaluación de la adhesión y mitigación de las debilidades

A medida que los debates nacionales sobre la adhesión al Protocolo cobran fuerza, es crucial que el contenido y las deficiencias de su texto se evalúen adecuadamente mediante un debate abierto y participativo. Esta última sección destaca los pasos y oportunidades relevantes que los Estados y las partes interesadas deberían considerar y promover como parte de este proceso participativo.

Evaluación de los impactos en los derechos humanos/en el marco legal y revisión constitucional

Además del análisis a priori por parte de las entidades legislativas y/o administrativas competentes de la observancia del Protocolo a la constitución del país, los debates nacionales sobre la adhesión o no al Protocolo deberían incluir una evaluación adecuada del impacto legal y sobre los derechos humanos llevada a cabo por las instituciones estatales facultadas para aprobar y ratificar acuerdos internacionales. Estas evaluaciones deben incluir una participación amplia y efectiva de todas las partes interesadas, incluidas las organizaciones de la sociedad civil de derechos humanos y digitales. Es fundamental que estas evaluaciones tengan en cuenta no solo la legislación nacional y las salvaguardias que se verían afectadas, sino también las obligaciones de los Estados en virtud del derecho internacional de los derechos humanos. Asimismo, el análisis de la constitucionalidad del Protocolo debe prestar especial atención a los principios aplicados a las relaciones y la cooperación internacionales, así como a las salvaguardias constitucionales en materia de privacidad y protección de datos (incluidas las competencias institucionales de las autoridades de supervisión). De este modo, los gobiernos estarán mejor equipados para evaluar la pertinencia de ratificar el Protocolo y, en su caso, las reservas y declaraciones a invocar. Estarán mejor equipados también para considerar las reformas legislativas resultantes de la adhesión de manera a no socavar los derechos humanos y las protecciones constitucionales.

En caso de adopción, reservas y declaraciones importantes al texto del Protocolo

El artículo 19 indica todo el conjunto de reservas y declaraciones mencionadas en el texto del Protocolo y cuándo invocarlas. A continuación enumeramos las que recomienda específicamente esta guía, que sirven para mitigar las deficiencias del Protocolo:

Artículo 7, párrafo 9(a) - permite a las Partes reservarse el derecho de no aplicar el artículo 7 para las solicitudes transfronterizas, convirtiendo así el artículo 8 en la base principal por la que se accede a los datos de los abonados en contextos transfronterizos. Una Parte que se reserve a este artículo no puede dictar

requerimientos directos de cooperación según el apartado 1 del artículo 7 del Protocolo a los proveedores de servicios en los territorios de otros signatarios.

Alternativamente,

Artículo 7, párrafo 2(b) - una Parte puede declarar que los requerimientos emitidos a los proveedores de servicios en su territorio "deben ser dictados por un fiscal u otra autoridad judicial, y estar bajo su supervisión, o ser dictado bajo supervisión independiente".

Artículo 7, párrafo 5 (a) y (b) - permite a una Parte exigir la *notificación* simultánea a sus autoridades nacionales cuando se dicta un requerimiento directo de cooperación y/o ordenar a los proveedores de servicios que *consulten a* las autoridades de la Parte antes de la revelación de la información relativa a abonados. Entre ambas posibilidades, la exigencia de notificación simultánea es la más adecuada para la protección de los derechos humanos en requerimientos transfronterizos directos.

Artículo 7, párrafo 5(e) - estipula que las Partes deben designar una sola autoridad para recibir dichas comunicaciones y realizar las actuaciones correspondientes. Para garantizar un mayor nivel de protección, las Partes deberían designar a una autoridad judicial independiente para que cumpla esta función.

Artículo 7, párrafo 9(b) - permite a las Partes reservarse el derecho de no aplicar el artículo 7 a ciertos tipos de números de acceso (ej. direcciones IP). Una Parte que haga esta reserva no podrá emitir requerimientos directos de cooperación para dichos números a los proveedores de servicios en los territorios de otras Partes.

Otros artículos:

Artículo 8, párrafo 4 - Las Partes pueden exigir información de apoyo adicional para procesar los requerimientos para la presentación rápida de información relativa a abonados y datos relativos al tráfico.

Artículo 12, párrafo 3 - Las Partes pueden exigir que su autoridad central sea signataria o intervenga de otro modo en el acuerdo por el que se crean los equipos conjuntos de investigación.

Esta no pretende ser una lista completa de todas las oportunidades relevantes de reservas y declaraciones en el texto del Protocolo. Hay otras posibilidades, y los países deben examinarlas al decidir si se adhieren al Protocolo y al evaluar su impacto en la legislación nacional existente y en las obligaciones del Estado en materia de derechos humanos.

Salvaguardias adicionales

1. Sobre la protección de datos. Adhesión al Convenio 108/108+

El Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108), con su protocolo modificador de 2018 (Convenio 108+)[75], es una referencia internacional influyente y fundamental en materia de protección de datos personales, con salvaguardias sólidas necesarias para lograr el debido equilibrio entre los poderes de aplicación de la ley y las salvaguardias de los derechos humanos. En la exposición de motivos del Protocolo se afirma que sus salvaguardias complementan las del Convenio 108, pero son pocos los países latinoamericanos que son parte de este Convenio. Los debates nacionales sobre la adopción del Protocolo son un momento clave para evaluar la oportunidad de que los Estados sean invitados a adherirse o solicitar la adhesión al Convenio 108/108+ del CdE[76].

2. Sobre la privacidad. Garantizar fuertes salvaguardias en la legislación nacional

Los Estados también deben establecer, o asegurarse de preservar, fuertes salvaguardias de la privacidad en sus marcos legales nacionales. Aunque esto no resuelve necesariamente los principales problemas del artículo 7, ayuda a aumentar el nivel de protección de la privacidad y a contrarrestar la influencia negativa del Protocolo para rebajar los niveles de privacidad, especialmente cuando se trata de la información relativa a abonados.

Enumeramos una serie de salvaguardias que los Estados, y los responsables de la toma de decisiones, deberían tener en cuenta:

- 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

[75] Informe Explicativo del Protocolo, párrafo 23.
[76] Véase más información sobre la adhesión al Convenio 108 por parte de Estados que no son miembros del Consejo de Europa, https://rm.coe.int/16809028a4.

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.