Nuevo Protocolo al Convenio sobre la Ciberdelincuencia en LatAm: Desafíos y estrategias de mitigación

Ahora y durante los próximos meses, los países elegibles para adherirse al Protocolo adicional segundo al Convenio sobre la Ciberdelincuencia del Consejo de Europa probablemente articularán debates nacionales para su adopción. Abierto a la firma el 12 de mayo de 2022, el Protocolo establece procedimientos que buscan reforzar la cooperación internacional para el acceso de las fuerzas de seguridad a los datos a través de las fronteras y plantea importantes retos para los derechos humanos y las libertades fundamentales. Las organizaciones de la sociedad civil, los activistas y los expertos que trabajan en la intersección de la tecnología y los derechos humanos pueden desempeñar un papel fundamental a la hora de garantizar que se preste la debida atención a estos retos, promover medidas de mitigación en caso de adhesión y fomentar la participación efectiva de todas las partes interesadas.

Aquí proporcionamos una hoja de ruta de incidencia para ayudar a los actores de la sociedad civil en ese frente. Se puede encontrar información más detallada sobre el Protocolo en nuestra guía *Evaluando el nuevo Protocolo al Convenio sobre Ciberdelincuencia en América Latina*.

Principales preocupaciones:

- El Protocolo exige a los Estados Parte que adapten su legislación para autorizar a las autoridades competentes (ej., la policía y la fiscalía) a requerir información relativa a abonados, como el nombre o la dirección de una persona, a un proveedor de servicios situado en otro territorio. Los procedimientos estándar de los artículos

6 y 7 no cuentan con la evaluación de una autoridad central o judicial en el territorio donde se encuentra el proveedor.

- No existe ningún mecanismo que garantice que los requerimientos directos de cooperación sean dictados por una autoridad judicial o de otro tipo independiente de las que llevan a cabo la investigación en el Estado Parte requirente.

- Confiar principalmente en los proveedores de servicios para evaluar las implicaciones de los requerimientos directos extranjeros para los derechos humanos y las libertades fundamentales puede socavar los derechos y las garantías consagrados en la legislación nacional del lugar donde se encuentra el proveedor de servicios (ej., el control judicial, los privilegios/inmunidades).

- Los procedimientos de cooperación directa del Protocolo entre las autoridades y los proveedores de servicios en el territorio de otra Parte parten de la suposición errónea de que la información relativa a abonados es intrínsecamente menos sensible y privada que otros tipos de datos de comunicaciones y "no permite sacar conclusiones precisas sobre la vida privada y los hábitos cotidianos de las personas afectadas". Por el contrario, los datos relativos a abonados son clave para identificar a las personas usuarias y vincularlas a sus actividades en línea.

- La preocupante formulación del Protocolo sobre la información relativa a abonados puede influir en los marcos jurídicos latinoamericanos sobre la privacidad para reducir la protección aplicada en la revelación de este tipo de datos.

- El Protocolo presenta un desequilibrio general entre las facultades de investigación y acceso a datos que los Estados Parte están *obligados* a asegurar y las salvaguardias de los derechos humanos que son *opcionales* o *prescindibles*.

- El Protocolo contiene salvaguardias de protección de datos más débiles en comparación con otros estándares internacionales ya establecidos.

Puntos a destacar:

- La información relativa a abonados es crucial para la identificación de las personas usuarias y puede revelar sus actividades, expresiones, relaciones y movimientos. Puede ser la punta del iceberg, revelando un perfil detallado sobre alguien. Nuestra Guía pone de relieve cómo la falta de salvaguardias adecuadas a la hora de revelar información sobre los suscriptores pone en peligro a los activistas, los defensores de los derechos humanos, los disidentes, los periodistas y la gente corriente.

- ¿Qué protecciones pueden ser socavadas por los requerimientos directos de cooperación en comparación con las salvaguardias legales nacionales y los principios básicos de la asistencia judicial internacional? (ej., la autorización judicial, los privilegios/inmunidades, las condiciones o los motivos de denegación que se aplicarían si la información del suscriptor se solicitara a través de la asistencia mutua).

- Cómo las salvaguardias de protección de datos del Protocolo se quedan cortas con respecto a referencias internacionales más protectoras (y a las normas nacionales

más estrictas, en su caso), y pueden eludirse a través de otras disposiciones del Protocolo.

Reivindicaciones a tener en cuenta:

- Además del análisis de la observancia del Protocolo a la constitución del país, abogar por evaluaciones del impacto del Protocolo sobre los derechos humanos y sobre leyes nacionales con una participación amplia y efectiva de todas las partes interesadas.

- Abogar por reservas y declaraciones importantes en caso de adhesión al Protocolo (véase nuestra Guía).

- Emparejar los debates sobre si el Estado se convertirá en Parte del Protocolo con la evaluación de la oportunidad de que el Estado sea invitado a adherirse o solicite la adhesión al Convenio 108/108+ del Consejo de Europa, que proporciona salvaguardias más sólidas en materia de protección de datos.

- Asegurar salvaguardias sólidas en la legislación nacional en caso de reformas legales resultantes de la aplicación nacional del Protocolo.

Partes interesadas a involucrar en el debate:

- *Actores gubernamentales/ estatales:* organismos gubernamentales responsables de la salvaguarda de los derechos humanos y fundamentales, y de los derechos de los consumidores; autoridades de protección de datos; asociaciones de jueces.

- *Sociedad civil:* expertos en protección de datos, organizaciones de consumidores que trabajan en la protección de datos, organizaciones de derechos humanos que trabajan en la justicia penal, abogados penalistas.

- *Empresas:* servicios de registro de nombres de dominio, empresas de telecomunicaciones y proveedores de servicios de Internet.