Asociación por los Derechos Civiles

6ª Ronda de Consultas sobre el 2º Protocolo adicional al Convenio de Budapest sobre cibercrimen

La Asociación por los Derechos Civiles (ADC) es una organización de la sociedad civil fundada en 1995 para defender y promover los derechos fundamentales en Argentina y América Latina, con especial atención a las necesidades de las personas en situación de vulnerabilidad por su género, nacionalidad, religión, condición de discapacidad, entre otras.

Celebramos esta nueva oportunidad de aportar comentarios, y antes de pasar a las observaciones, queremos agradecer el trabajo realizado por la Comisión, así como por abrir estos espacios de participación ciudadana. En el mismo sentido, queremos destacar especialmente la inclusión de un capítulo sobre las garantías y condiciones relativas a la protección de datos personales.

Ahora queremos aprovechar esta nueva ronda para profundizar en las observaciones anteriores que aún no han sido resueltas y abordar los temas nuevos añadidos al protocolo.

a. Sección 2: Procedimientos que mejoran la cooperación internacional entre autoridades para la divulgación de datos informáticos almacenados

Art. 6: Solicitud de información de registro de nombres de dominio y art. 7: Revelación de información sobre los usuarios

Como se señala en el informe explicativo en el párrafo 93, esta sección pretende encontrar un mecanismo rápido y eficaz de cooperación en el que las autoridades de una Parte puedan solicitar información de registro de nombres de dominio y de abonados a entidades privadas situadas en el territorio de otra Parte. Si bien esta

información podría obtenerse a través del MLA (Mutual Legal Assistance) del procedimiento fijado en el artículo 18 del Convenio, se consideró importante establecer este mecanismo complementario que permita un acceso transfronterizo más eficaz a la información necesaria para investigaciones o procedimientos penales específicos.

Aunque estamos de acuerdo con la necesidad de contar con mecanismos ágiles y competentes que permitan una investigación criminal efectiva, guardamos ciertas reservas en cuanto a la autoridad que debe estar facultada para llevar a cabo tales actuaciones.

Autoridad competente

Tanto el procedimiento del artículo 6 como el del 7 establecen que la solicitud puede ser emitida por la autoridad competente designada por la Parte. A su vez, el artículo 3.2.b define "autoridad competente" como una “autoridad judicial, administrativa u otra autoridad encargada de hacer cumplir la ley que este facultada por el derecho interno para ordenar, autorizar o llevar a cabo la ejecución de medidas en virtud del presente Protocolo con el fin de obtener o presentar pruebas en relación con investigaciones o procedimientos penales específicos.”

Como esta sección se aplica independientemente de que exista un tratado o acuerdo de asistencia mutua o no entre la Parte que solicita la información y la Parte en cuyo territorio se encuentra la entidad privada, la intervención de una autoridad judicial independiente o de naturaleza similar es esencial para controlar la legalidad en el proceso y proteger los derechos individuales. Como ya dijimos en comentarios anteriores, la adopción de un criterio de autoridad amplio para el dictado de medidas con escasas salvaguardas es sumamente riesgosa para los derechos de las personas. Bajo esta norma, las autoridades locales o municipales, la policía o

cualquier persona que el Estado-parte determine libremente tendrán legitimidad para comunicarse directamente con el proveedor de servicios y obligarle a proporcionar información sensible. De ese modo, pueden darse situaciones en las que el acceso o la transferencia de datos se produzca sin la intervención de ningún organismo público independiente capaz de evaluar la legalidad de la orden.

A este respecto, el artículo 7.2.b establece la posibilidad de que cada Parte declare que la orden prevista en el artículo 7.1 debe ser emitida por un fiscal u otra autoridad judicial, o bajo su supervisión, o de lo contrario ser emitida bajo una supervisión independiente. Sugerimos, para garantizar un control legal mínimo, que esta disposición sea obligatoria para todos los procedimientos de la Sección II.

Información de los abonados

Entendemos que la definición de información de los abonados utilizada en el convenio[1] abre la posibilidad de que el concepto incluya información sensible, por lo cual el requisito de una autoridad judicial o independiente cobra especial relevancia.

De este modo, insistimos en que la claridad en la definición del término es vital para distinguir información que es menos intrusiva para la privacidad de la que supone un grave riesgo para la misma. En ese sentido, mantenemos nuestra preocupación expuesta en comentarios anteriores sobre el riesgo de que se incluyan datos que revelen comportamientos, hábitos u otras características de la vida privada de una persona en esta categoría. En particular, las direcciones IP no deberían incluirse como "información de los abonados". Por ejemplo, cuando son suministradas por proveedores distintos de los que prestan el servicio de telecomunicaciones, las direcciones IP constituyen datos de tráfico en la medida de que forman parte de la información producida dentro de – y referida a – la comunicación realizada por la

[1] art. 18.3 de la convención y el párrafo 92 del informe explicativo

persona con un usuario o con un servicio determinado. Pero incluso cuando esta información es proporcionada por el ISP, puede revelar detalles íntimos sobre la ubicación, las costumbres o las acciones cotidianas de una persona[2]. Por lo tanto, la cuestión importante no es si algún dato puede o no considerarse "información de los abonados", sino en qué medida puede suponer un grave riesgo para el derecho a la intimidad. En este sentido, el Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos consideró que la vigilancia selectiva está "generalmente amparada en procesos penales o algún otro tipo de investigaciones, e implica la recolección y/o monitoreo de las comunicaciones de un individuo identificado o identificable, y de una dirección IP, un dispositivo específico, una cuenta específica, etc.[3]"Por lo tanto, tales medidas constituyen una "interferencia en la privacidad del individuo"[4] y su legitimidad debe ser considerado sobre la base de la prueba tripartita, que establece que la medida debe ser legal, necesaria para una sociedad democrática y proporcionada. En virtud de este principio, las direcciones IP deben exigirse siempre por orden judicial.

Aunque el art. 9.b reconoce este posible problema y permite a las Partes hacer una reserva al respecto, entendemos que no debería ser una facultad de ellas sino una limitación expresa para proteger los derechos de las personas.

b. Sección 3: Procedimientos que mejoran la cooperación internacional entre autoridades para la divulgación de datos informáticos almacenados

[2] ‘’What an IP address can reveal about you’’. Informe elaborado por la Subdivisión de Análisis Tecnológico de la Oficina del Comisionado de Privacidad de Canadá, mayo de 2013. Disponible en https://www.priv.gc.ca/media/1767/ip_201305_e.pdf
[3] Estándares para una Internet libre, abierta e inclusiva. Comisión Interamericana de Derechos Humanos. Disponible en http://www.oas.org/en/iachr/expression/docs/publications/INTERNET_2016_ENG.pdf
[4] Ibid., párrafo 215.

Art. 9 Divulgación acelerada de datos informáticos almacenados en caso de emergencia

El canal establecido en este artículo pretende ser un mecanismo más rápido y sencillo para cooperar en caso de emergencia. Entre las características que lo hacen más expeditivo está el hecho de que no es necesario que se prepare una solicitud de asistencia mutua previamente.

Según el Informe Explicativo en el párrafo 153, corresponde a las Partes decidir el uso de este nuevo canal o de la MLA *solicitud de asistencia mutua en caso de emergencia*, basándose en su experiencia acumulada y en las circunstancias específicas de hecho y de derecho. Sin embargo, esta decisión asume incorrectamente que la elección es sólo una cuestión de conveniencia. En realidad, el proceso de la MLA exige ciertos pasos formales – por ejemplo, solicitudes previas de asistencia mutua – que exigen el cumplimiento de unas garantías mínimas. Por el contrario, el intercambio de información en tiempo real puede permitir a los Estados parte evitar el cumplimiento de las normas de protección de datos u otros derechos fundamentales fácilmente. Por lo tanto, el protocolo debe reconocer que este nuevo canal es más exigente – en términos de salvaguarda de derechos – que la MLA. De tal modo, la elección no debe depender de la discrecionalidad de los Estados, sino de que la situación de emergencia reúna unas condiciones que la diferencien de la que normalmente autoriza el uso de la MLA. Tales cualidades pueden darse exigiendo que la inminencia o el riesgo sean imperativos o apremiantes.

Otra forma sería exigir que el Estado solicitante tenga que demostrar que es imposible o inútil utilizar la vía de la MLA debido a la sensibilidad del caso. Por la misma razón, sólo una autoridad judicial o similar independiente debería tener la facultad de emitir dicha solicitud.

c. Sección 5 Procedimientos relativos a la cooperación internacional en ausencia de acuerdos internacionales aplicables

Art. 12 Equipos conjuntos de investigación e investigaciones conjuntas

El Art. 12 establece que la decisión de crear o unirse a un equipo conjunto de investigación (en inglés Joint Investigation Teams) será tomada por la "autoridad competente" determinada por cada Estado Parte. Si bien esta disposición puede estar fundamentada en la diversidad de los sistemas jurídicos, consideramos que no es razón para impedir que el protocolo solicite que dicha autoridad sea una autoridad judicial u otra con el mismo grado de independencia. Los acuerdos para poner en marcha los ECI son muy delicados porque definen las condiciones y procedimientos de las operaciones y, por tanto, pueden afectar a los derechos fundamentales de las personas. Por lo tanto, se debe contar con una fuerte supervisión sobre la necesidad y legitimidad de la operación, que debe ser llevada a cabo por un juez o alguna otra autoridad imparcial.

Además, el protocolo debe exigir que los fines de los acuerdos estén redactados de la manera más clara, detallada y específica, en caso que surja duda sobre la interpretación de un término, la respuesta debería ser restringir el uso de las pruebas a otros usos o casos diferentes.

d. Capítulo III Condiciones y salvaguardias

Aunque los artículos 13 y 14 establecen condiciones y salvaguardias que incluyen protección de los datos personales, sugerimos que se exijan más requisitos para preservar los derechos de las personas.

Además de esto, existen salvaguardias que pueden ser agregadas a la Convención, como las siguientes:

-Solicitar a todos los estados parte la aprobación de una ley de protección de datos de acuerdo con altos estándares internacionales. El Convenio 108 y el 108+ serían apropiados para este fin.

-Permitir el acceso a la revisión previa de los datos por un tribunal judicial u otra autoridad independiente e imparcial.

-Solicitar la notificación a la persona a cuyos se han accedido, en la medida en que no se ponga en peligro la investigación. Si ese es el caso, el individuo debe ser informado inmediatamente una vez que haya cesado el peligro. En este sentido, el artículo 14.11 establece la necesidad de transparencia y notificación. Sin embargo, el descargo de responsabilidad sobre las "restricciones razonables según su marco jurídico interno" debería aclararse para evitar restricciones abusivas.

Por último, la reciente adopción de la Observación General 25 (2021) sobre los derechos del niño en relación al entorno digital nos obliga a poner atención en la protección de los datos de menores sujetos a investigación penal. Por esta razón, sugerimos que el protocolo considere esta nueva situación introduciendo salvaguardias específicas. En este sentido, puede ser relevante el párrafo 47 de la Observación General 25 que establece:

“Las tecnologías digitales aportan una complejidad adicional a la investigación y el enjuiciamiento de los delitos cometidos contra niños, que pueden ser de carácter transnacional. Los Estados partes deben examinar las modalidades en que la utilización de las tecnologías digitales puede facilitar u obstaculizar la investigación y el enjuiciamiento de los delitos cometidos contra niños y adoptar todas las medidas preventivas, coercitivas y correctivas disponibles, en cooperación con asociados internacionales cuando proceda. Deben impartir formación especializada a los agentes del orden, a los fiscales y a los jueces en relación con las vulneraciones de

los derechos del niño específicamente relacionadas con el entorno digital, entre otras formas mediante la cooperación internacional.”

Para más información, póngase en contacto con Valeria Milanes, Directora Ejecutiva, vmilanes@adc.org.ar , Alejo Kiguel, Oficial de Proyectos Ssr, akiguel@adc.org.ar , o Eduardo Ferreyra, Oficial de Proyectos Ssr, eferreyra@adc.org.ar