

CONSERVACIÓN DE DATOS DE TRÁFICO EN PARAGUAY



CONSERVACIÓN DE DATOS DE TRÁFICO EN PARAGUAY

TEDIC es una Organización No Gubernamental fundada en el año 2012, cuya misión es la defensa y promoción de los derechos humanos en el entorno digital. Entre sus principales temas de interés están la libertad de expresión, la privacidad, el acceso al conocimiento y género en Internet.

CONSERVACIÓN DE DATOS DE TRÁFICO EN PARAGUAY

OCTUBRE DE 2023

RESPONSABLE DEL ANÁLISIS LEGAL Y REDACCIÓN

Maricarmen Sequera Buzarquis

COMUNICACIÓN

Araceli Ramírez

DIAGRAMACIÓN

Horacio Oteiza



Esta obra está disponible bajo licencia Creative

Commons Attribution 4.0 Internacional (CC BY SA 4.0)

<https://creativecommons.org/licenses/by-sa/4.0/deed.es>

TABLA DE CONTENIDO

INTRODUCCIÓN	5
¿LA CONSERVACIÓN DE DATOS DE TRÁFICO RESUELVE LOS HECHOS PUNIBLES?	6
¿QUÉ DICE LA NUEVA LEY PYRAWEBOS Y QUÉ RIESGOS IDENTIFICAMOS?	7
1. Falta de garantías y resguardos legales de la información personal	7
2. Autoridad competente para la protección y monitoreo del tratamiento de datos	7
3. Autorización judicial y aplicación del test de necesidad, idoneidad y proporcionalidad de la medida en relación con el fin perseguido	7
4. Cumplimiento del debido proceso sobre los metadatos y cuáles metadatos	8
5. Limitaciones de la configuración de Internet en Paraguay	8
6. Limitar el uso de la conservación de datos de tráfico solo para ciertos hechos punibles	9
7. La privacidad y las respuestas internacionales (ONU y EU)	9
CONSIDERACIONES FINALES	10

INTRODUCCIÓN

En octubre de 2022, ingresó a la Cámara de Diputados el proyecto de ley: “Que dispone la obligatoriedad de la conservación de datos de tráfico para combatir la pornografía infantil y hechos punibles conexos”, presentado por el Diputado Rodrigo Blanco, con el número de expediente D-2269521.

En ese mismo mes, la Comisión de Niñez, Juventud y Desarrollo aprobó el proyecto de ley sin realizar modificaciones. Por otro lado, en junio de 2023, la Comisión de Ciencia y Tecnología emitió un dictamen con algunas modificaciones. Sin embargo, aún están pendientes de emitir dictamen las Comisiones de Asuntos Constitucionales, Legislación y Codificación, Justicia, Trabajo y Previsión Social. Actualmente, el proyecto de ley se encuentra en estado de postergación.

¿LA CONSERVACIÓN DE DATOS DE TRÁFICO RESUELVE LOS HECHOS PUNIBLES?

Es crucial evitar caer en la falacia de que la propuesta legislativa en cuestión resolverá casos de crímenes como la pornografía infantil, el narcotráfico, el lavado de activos y el terrorismo. En los países de la región que ya han implementado normativas similares, no necesariamente se ha logrado una disminución o resolución de estos delitos exclusivamente a través de la retención de datos. Se debe considerar que la identificación de individuos involucrados en delitos o crímenes debe enfocarse hacia el futuro en lugar de revisar el pasado.

Abrir la puerta a la vigilancia masiva es inaceptable, ya que esta práctica es ilegal, desproporcionada y carece de justificación. La persecución de delitos debe llevarse a cabo únicamente cuando exista una sospecha fundamentada, se realice de manera individualizada y esté respaldada por un proceso legal. Esto es fundamental para no infringir principios esenciales como la presunción de inocencia, el derecho a la privacidad y la libertad de expresión, incluso en el entorno digital.

En otros países, por ejemplo, cuando se detecta la subida de una imagen de pornografía infantil a la web, se procede a identificar la dirección IP (usuario) asociada a dicha actividad. A partir de ese punto, y solo bajo una causa legal válida, se conservan los datos pertinentes relacionados con ese usuario con el propósito de supervisar su conducta. Esto se conoce como vigilancia específica y representa una alternativa efectiva para colaborar en la resolución de delitos, siempre que se respeten los principios de un debido proceso.

¿QUÉ DICE LA NUEVA LEY PYRAWEBBS Y QUÉ RIESGOS IDENTIFICAMOS?

El 1 de junio, se realizó una audiencia pública para discutir sobre esta ley. Nuestra directora, Maricarmen Sequera, participó activamente y compartió sus preocupaciones sobre la propuesta de ley, entre ellas:

1. FALTA DE GARANTÍAS Y RESGUARDOS LEGALES DE LA INFORMACIÓN PERSONAL

Paraguay, junto a Bolivia, son los únicos países de América del Sur que no cuentan con una ley de protección integral de datos personales. Esta ley será la base para justificar el almacenamiento y tratamiento de cualquier dato personal. Necesitamos una ley de protección que brinde garantías y control de la información personal depositada en sistemas de almacenamiento digital, asegurando que personas inescrupulosas que vendan y distribuyan cualquier dato de carácter personal sean llevadas a la justicia. No podemos debatir un proyecto de Retención de Datos sin antes contar con una Ley de Protección de Datos Personales. La clave será contar con una agencia independiente para actuar en caso de abusos y riesgos por parte de las instituciones del Estado, sector privado, academia, etc.

2. AUTORIDAD COMPETENTE PARA LA PROTECCIÓN Y MONITOREO DEL TRATAMIENTO DE DATOS

Será necesario crear un órgano independiente como ente rector y responsable del control del tratamiento de datos, para analizar la finalidad de los mismos y hacer revisiones preventivas de posibles errores o abusos que se den en los tratamientos de datos. Además, cualquier medida de restricción a la privacidad y el anonimato en Internet debe estar bajo control de un órgano autónomo y especializado, que tenga la capacidad para resguardar a los ciudadanos de cualquier amenaza a la integridad de sus comunicaciones. No vemos que eso esté resuelto en el proyecto que está a estudio del Congreso en Paraguay.

3. AUTORIZACIÓN JUDICIAL Y APLICACIÓN DEL TEST DE NECESIDAD, IDONEIDAD Y PROPORCIONALIDAD DE LA MEDIDA EN RELACIÓN CON EL FIN PERSEGUIDO

Se reconoce que en la propuesta actual se buscó incluir las garantías judiciales. En la propuesta actual incluye la autorización judicial, será clave que la interceptación de las comunicaciones a través de las retenciones de datos de tráfico sea debidamente justificada y argumentada por parte de un juez. Que el juez aplique previamente el test de proporcionalidad y necesidad para evaluar si esta herramienta tecnológica de retención de datos de tráfico, que pone en riesgo los principios fundamentales, es de última ratio y única forma de identificar y resolver el litigio ante el poder judicial.

4. CUMPLIMIENTO DEL DEBIDO PROCESO SOBRE LOS METADATOS Y CUÁLES METADATOS

Los metadatos que se recopilarán según la propuesta de ley son la identificación del protocolo de Internet. Sin embargo, no se especifica de manera detallada cuáles son las informaciones sujetas a retención. Es crucial que la propuesta de ley incluya una descripción precisa para evitar ambigüedades en la interpretación legal. Qué es etiqueta de localización? ¿Se considera la geolocalización del dispositivo? Acerca de la dirección del protocolo de Internet (IP): Esto se refiere a las direcciones IP que se utilizan para identificar dispositivos en la red, tanto el origen como el destino de los datos. Por lo general, se registran tanto la dirección IP de origen como la dirección IP de destino. En el 2015 habíamos realizado un video para explicar los riesgos que tiene esto.

Por ejemplo, la información como el número de teléfono que recibe una llamada, la duración de la llamada, la ubicación geográfica del dispositivo, así como sus identificadores únicos, tales como IMEI e IMSI en dispositivos móviles o fijos, y las direcciones IP en el contexto de Internet son datos denominados “Metadatos” de una comunicación. Es decir, información acerca de los datos de comunicación en lugar del contenido mismo de la comunicación. Un ejemplo ilustrativo de esta distinción sería considerar que los metadatos equivalen a los detalles exteriores de un sobre que contiene una carta, mientras que el contenido de la carta sería lo que se encuentra en su interior. Sin embargo, la clasificación de datos de esta manera podría llevar a una conclusión equivocada, la de que los metadatos o los datos de identificación del suscriptor merecen una protección menor en comparación con las propias comunicaciones. Contrariamente, la agregación de estos datos resulta ser, en realidad, más reveladora que el contenido de las comunicaciones en sí. Como señaló Edward Snowden, los metadatos son los que permiten un seguimiento minucioso y un registro preciso de todas las actividades privadas en nuestras vidas, ofreciendo una visión detallada de nuestras relaciones, nuestras afiliaciones políticas y nuestras actividades cotidianas.

5. LIMITACIONES DE LA CONFIGURACIÓN DE INTERNET EN PARAGUAY

El propósito fundamental de este proyecto de ley es abordar la cuestión de la «identificación» de posibles autores de un delito. En otras palabras, se busca establecer quiénes son los sospechosos de cometer un delito con base en las huellas digitales que dejan al conectarse a Internet. En este contexto, la responsabilidad de llevar a cabo dicha identificación recae en los proveedores de servicios de Internet (ISP), ya sean organizaciones o empresas. Es importante destacar que la problemática de identificación se origina en la peculiar configuración de Internet en Paraguay. Cuando un cliente contrata servicios de Internet, algunas ISP optan por no asignar una «IP pública» al cliente, con el fin de aumentar su rentabilidad en el negocio. En su lugar, proporcionan al usuario una «IP privada» que se encuentra enmascarada junto con las direcciones de aproximadamente otras 200 personas detrás de una «IP pública». Esto significa que, a diferencia de lo que sucede en la mayoría de los países, en Paraguay no se garantiza que cada servicio cuente con una «IP pública» única.

6. LIMITAR EL USO DE LA CONSERVACIÓN DE DATOS DE TRÁFICO SOLO PARA CIERTOS HECHOS PUNIBLES

Es imperativo restringir la aplicación de la retención de datos de tráfico exclusivamente a ciertos delitos. Si el propósito de la ley es combatir eficazmente delitos como la pornografía infantil y conexos, debe limitarse a ese ámbito y no extenderse a otros tipos de infracciones y crímenes. La ampliación de esta medida a cualquier delito o crimen, dadas las limitaciones de nuestro sistema judicial, podría abrir la puerta a que cualquier individuo presente acusaciones con el único fin de obtener acceso a toda la información y actividad en línea de otro. Por ejemplo, en casos de difamación y calumnia, esta extensión podría posibilitar que cualquiera presente una denuncia con el único objetivo de acceder a la información y luego retirarla o desestimarla.

En la propuesta actual modificada en el Congreso habla sobre “otros delitos informáticos”, esto amplía para casos de acceso indebido a un dispositivo, acceso indebido a datos, interceptación, preparación al acceso indebido a datos, alteración de datos, acceso indebido a sistemas informáticos, sabotaje a sistemas informáticos, alteración de datos relevantes, falsificación de tarjetas de crédito y débito y estafa mediante sistemas informáticos. ¿No les parece desproporcionado abrir la posibilidad de acceder a la vida digital de una persona para resolver este tipo de casos legales?

7. LA PRIVACIDAD Y LAS RESPUESTAS INTERNACIONALES (ONU Y EU)

Un ejemplo elocuente es la declaración del ex Relator Especial de las Naciones Unidas sobre la Libertad de Expresión y Opinión, Frank La Rue, quien en 2013 destacó que el análisis de los metadatos puede resultar sumamente revelador e invasivo, especialmente cuando estos datos se combinan y agregan. Además, señaló lo siguiente: «Las leyes nacionales que exigen la conservación de datos son intrusivas y costosas, y socavan los derechos a la privacidad y la libre expresión. Al obligar a los proveedores de servicios de comunicación a generar amplias bases de datos que contienen información sobre quién se comunica telefónicamente o a través de Internet, la duración de dichas comunicaciones y la ubicación de los usuarios, y a mantener esta información, a menudo durante largos períodos, las leyes de retención de datos obligatoria expanden significativamente el alcance de la vigilancia estatal y, por ende, el alcance de las violaciones de los derechos humanos. Estas bases de datos de comunicación se vuelven vulnerables al robo, el fraude y la divulgación accidental.» De hecho, el Tribunal de Justicia de la Unión Europea anuló una directiva comunitaria que había estado vigente desde 2006 y que obligaba a las compañías telefónicas y a otras empresas de comunicaciones electrónicas a retener los datos personales de los ciudadanos con fines de seguridad. En su fallo, el Tribunal de Justicia argumentó que la Directiva constituía una injerencia significativa en los derechos fundamentales, como el derecho al respeto de la vida privada y la protección de los datos personales. También señaló que la retención y el uso posterior de estos datos sin informar previamente a los abonados o usuarios registrados podía generar la percepción de que sus vidas privadas estaban siendo objeto de una vigilancia constante.

CONSIDERACIONES FINALES

Para nosotras en TEDIC, es fundamental reconocer que la retención de datos constituye una medida que limita y repercute en los derechos a la privacidad y a la libertad de expresión. La retención de datos de tráfico es una medida que involucra la recolección y almacenamiento de información como números de teléfono, duración de llamadas, ubicaciones y direcciones IP. A pesar de su uso en la lucha contra el crimen, esta práctica plantea preocupaciones significativas en cuanto a la invasión de la privacidad y la restricción de la libertad de expresión. El ex Relator Especial de la ONU sobre la Libertad de Expresión, Frank La Rue, ha advertido sobre la intrusividad y los riesgos de las leyes de retención de datos, que pueden dar lugar a un exceso de vigilancia y violaciones de derechos humanos. Además, el Tribunal de Justicia de la Unión Europea consideró que una directiva de retención de datos era una seria intrusión en los derechos fundamentales, incluyendo el respeto a la vida privada y la protección de datos personales. En este contexto, es fundamental que el Congreso Nacional analice minuciosamente cualquier propuesta de regulación de la retención de datos, asegurando que cumple con los estándares de legalidad, finalidad imperativa, necesidad, idoneidad, proporcionalidad de la medida en relación con el fin perseguido, autorización judicial y debido proceso. Persisten preocupaciones en torno a los conceptos ambiguos que rodean la retención de datos de tráfico, los tipos de metadatos que deben registrarse y los requerimientos del debido proceso, así como la necesidad de obtener una autorización judicial fundamentada antes de proceder con la retención. Es fundamental replantear la retención de datos de manera que se realice con miras al futuro, basada en la existencia de un delito, a fin de garantizar el pleno cumplimiento del debido proceso y de la vigilancia específica. Esta aproximación contrasta con la retención masiva de datos, que representa una amenaza para nuestros derechos a la privacidad y a la libertad de expresión. Más allá de estos aspectos, se debe priorizar la sanción de una propuesta legislativa integral de protección de datos personales, que garantice un equilibrio adecuado entre la seguridad y la privacidad de las personas. La regulación de la retención de datos debe ser cuidadosamente considerada, teniendo en cuenta sus implicaciones en los derechos fundamentales, y no debe llevarse a cabo a expensas de la privacidad y la libertad de expresión de las personas.

