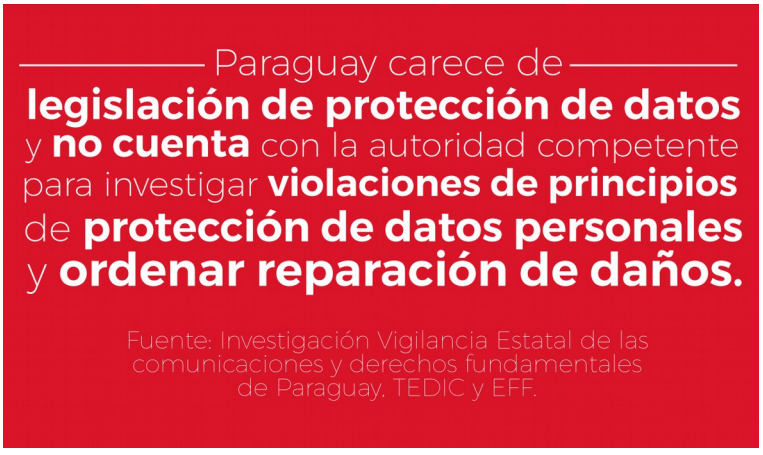
Paraguay

¿Cuál es el marco legal que protege la privacidad en Paraguay?

Paraguay está sujeto a tratados internacionales en materia de derechos humanos. Estos tratados, como la Convención Americana sobre Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos, reconocen el derecho a la privacidad y otras libertades fundamentales. Estos tratados son obligaciones internacionales asumidas por el Estado y son aplicables en el derecho interno.

A nivel nacional, el articulo 33 de la constitución también reconoce el derecho a la intimidad y privacidad. El articulo 36 protege el derecho a la inviolabilidad de patrimonio documental y la comunicación privada. Este derecho protege el secreto de las comunicaciones y el derecho a la integridad de las comunicaciones. La protección de datos también se encuentra protegida en el artículo 135 de la Constitución.

¿Mis derechos están protegidos frente a la vigilancia estatal de las comunicaciones?



Adicionalmente a la protección constitucional, el Código Penal, Ley N° 1160/97 establece sanciones entre dos años y multa para el que intercepte, oiga, grabe, almacene o facilite la intercepción de comunicaciones de un tercero y las mismas sanciones para el que difunda imágenes de otra persona que pueda violar su privacidad o intimidad.

Respecto al secreto de las comunicaciones, el Articulo 146 establece que el que viola el secreto de las comunicaciones o correspondencia dirigidas a terceros debe cumplir con una pena de hasta un año o con una multa. Lamentablemente, Paraguay no cuenta con una ley de protección de datos personales que sea realmente exhaustiva.

TEDIC

ELECTRONIC FRONTIER FOUNDATION

¿Cual es el marco legal que autoriza al estado vigilar mis comunicaciones?

Los artículos 25 al 27 del CP definen tanto los actos (intervención de comunicaciones telefónicas, radiales, correspondencia, sistemas y redes informáticas y demás comunicaciones, definidos en el art. 25) como los mecanismos legales necesarios y los procedimientos a seguir posteriormente.

> *Artículo 26.- "Autorización judicial. Será competencia del Secretario Nacional de Inteligencia, solicitar la autorización judicial para emplear los procedimientos señalados en el artículo anterior. La solicitud deberá ser formulada ante el Juez Penal de Garantías de Turno del lugar en el cual se habrá de realizar el procedimiento respectivo.*
>
> *El Juez podrá o no ordenar, por resolución fundada, bajo pena de nulidad, la realización de los procedimientos a que se refiere el artículo anterior, dentro del plazo de 24 (veinticuatro) horas, sin más trámite. La resolución que la ordene, deberá especificar los medios que se emplearán, la individualización de la o las personas a quienes se aplicará la medida y el plazo por el cual se decreta, que no podrá ser superior a 90 (noventa) días, prorrogable por una sola vez hasta por igual período".*
>
> *Artículo 27. – "Examen. El Secretario Nacional de Inteligencia deberá entregar el resultado del procedimiento al Juez que lo ordena, quien procederá a escuchar para sí el contenido, y también podrá ordenar la versión escrita de la grabación o de aquellas partes que considere útiles y ordenará la destrucción de toda la grabación o de las partes que no tengan relación con el procedimiento, previo acceso a ellas".*

Resumiendo, el CP deja claro que para suspender la protección de la privacidad de las comunicaciones por parte de las agencias de inteligencia deben cumplirse los siguientes cinco supuestos:

1. Excepcionalidad e indispensabilidad de la interceptación de las comunicaciones de que se trate
2. Medida a tomar únicamente cuando la interceptación tiene relación con bienes jurídicos o intereses estatales establecidos en la norma;
3. Autorización judicial requerida bajo pena de nulidad;
4. Identificación precisa de la/s persona/s a ser investigadas (prohibición de interceptaciones masivas o innominadas);
5. Tiempo limitado de la investigación de inteligencia.

Adicionalmente existen otras normativas que incluyen referencias a la vigilancia:

- Ley especial sobre represión al tráfico de drogas y estupefacientes (art. 88, 89, 91 en casos específicos.

Las interceptaciones de comunicación establecidas en la norma se encuentran en el capítulo relativo a las "Entregas vigiladas" y a las "Operaciones encubiertas" cumpliendo los siguientes supuestos:

1. Necesidad de autorización judicial en cada caso;
2. Excepcionalidad de la interceptación de comunicaciones y correspondencia;

3. Señalamiento concreto del tipo de comunicación que se quiere interceptar;
4. Pertinencia de la interceptación (qué se pretende lograr con la misma);
5. Posibilidad de que el juez solicite razones adicionales para el dictado de la medida, si lo considera necesario;
6. Claridad en los limites del tiempo de la interceptación;
7. El control y el seguimiento de cada operativo e investigación estarán a cargo del juez y del fiscal respectivo;
8. Obligación de quienes participan en los operativos ("Entregas vigiladas" u "Operaciones encubiertas") de guardar estricta reserva y respetar la intimidad de las personas.

Adicionalmente la Ley de comercio electrónico (Ley 4868/13) contempla en su artículo 10 que las empresas proveedoras de internet en paraguay y las que proveen alojamiento de datos deben almacenar como mínimo 6 meses los datos de tráfico o "relativos a la comunicaciones electrónicas".

La ley no cuenta con los estándares mínimos para salvaguardar la información privada de los usuarios, ni criterios para justificar más datos de lo que la empresa privada necesita. Este artículo limita al poder judicial y policial a acceder a los datos almacenados por las empresas.

¿Quiénes y cómo pueden vigilar mis comunicaciones?

El gráfico explica el procedimiento para intervenir una comunicación en material penal:

Adicionalmente, los servicios de inteligencia pueden interceptar comunicaciones también mediante un procedimiento que se inicia con una investigación de la Secretaría Nacional De Inteligencia Criminal y una solicitud de obtención de información de parte de la misma institución, el juzgado de garantías puede autorizar o no esta solicitud, en el caso que sea positiva el juzgado debe controlar la interceptación.

¿Están las empresas de telecomunicaciones obligadas a retener mis comunicaciones? ¿Bajo que condiciones la policía puede acceder a los datos de mi comunicación?

No, el proyecto de ley de conservación obligatoria de datos de tráfico fue rechazado en el Congreso. Sin embargo, la ley 4868/13 de Comercio Electrónico, en su artículo 10[1] obliga a las empresas telecomunicaciones a almacenar como mínimo 6 meses los datos "relativos a la comunicaciones electrónicas". Este artículo prohíbe al poder judicial y policial a acceder a aquellos datos retenidos en material penal.

¿Puede el estado realizar ataques maliciosos para vigilar mis comunicaciones?

El escenario legal es incierto. No existe una regulación específica que faculte a autoridades el llevar a cabo ataques maliciosos para vigilar las comunicaciones de una persona.

En principio aplicarían las reglas que existen respecto de cualquier intervención de comunicaciones privadas, El artículo 200 del Código de Procedimiento Penal establece que un juez puede ordenar la interceptación de las comunicaciones de los acusados, con "independencia de los medios técnicos utilizado para lograrlo," un poder sorprendentemente amplio, teniendo en cuenta las numerosas maneras que la nueva tecnología puede ser utilizada para espiar en los ciudadanos. En todos los casos sería necesaria una autorización judicial para llevar a cabo este tipo de medidas.

Adicionalmente, en nuestra opinión, sería necesaria una autorización específica en una ley para poder utilizar este tipo de prácticas y únicamente cuando no exista una medida menos gravosa para llevar a cabo una intervención de comunicaciones privadas. El estado Paraguayo ha adquirido sofware malicioso Finfisher.

¿Es legal usar cifrado?

Sí, no existe legislación o práctica que prohíba el uso del cifrado.

¿Cómo me entero si el estado vigila mis comunicaciones?

En Paraguay no existe ninguna obligación de notificar a la persona sujeta a la vigilancia de sus comunicaciones, por lo que es muy difícil para una persona conocer esta situación y ejercer su derecho de defensa. En ese sentido, es necesaria la incorporación del derecho de notificación al usuario. Concretamente; si una autoridad recibe facultades de vigilancia por alguna ley, ésta debe reconocer el derecho de las personas a conocer que han sido sujetos de vigilancia. Esta notificación solamente debe diferirse sí, y solo sí, el juez encargado de otorgar la autorización determine que la notificación pondría en riesgo la consecución del interés legítimo. En todo caso, la ley debe fijar plazos máximos para el diferimiento de la notificación.

La notificación debe detallar todo el material obtenido por la autoridad, producto de la vigilancia, de manera que la persona afectada pueda conocer el contenido y alcance de la invasión de su privacidad y pueda, en consecuencia, ejercer

1 Ley 4868/13 de *Comercio Electrónico*. Disponible en: http://www.eljurista.com.py/admin/publics/upload/archivos/ea41b40fb8ce27bd7ec64237fd75ef89.pdf Fecha de consulta: 2 de Diciembre, 2015].

su derecho de acceso a la justicia para remediar cualquier abuso.

¿Cuántas comunicaciones han sido interceptadas por el Estado paraguayo?

Las normas que regulan la vigilancia de comunicaciones no obligan a presentar reportes de transparencia, ni para los proceso penales ni para las labores de inteligencia. En los informes anuales de la Policía Nacional, el Ministerio Público y la SENAD no son publicados el número de solicitudes aprobadas y rechazadas, ni tampoco un desglose de las solicitudes por proveedor de servicios, por autoridad, tipo y propósito.

¿El Estado paraguayo ha mostrado interés en proteger la privacidad de los ciudadanos?

En Paraguay no existe información suficiente sobre el uso de herramientas de vigilancia por parte del estado. Las leyes paraguayas no obligan al estado a emitir reportes de transparencia con relación al número de solicitudes de vigilancia que realiza la policía como los servicios de inteligencia. Tampoco presentan una tutela efectiva, ni cuenta con un organismo que supervise las actividades de vigilancia. No cuenta con una ley de protección de datos personales, del mismo modo no existen las garantías necesarias para la protección de los usuarios frente a los abusos o la violación de la confidencialidad de las comunicaciones, de conformidad con las obligaciones estatales en materia de derechos humanos. El único mecanismo a disposición es el Habeas Data, que es insuficiente.

Sin embargo, debemos rescatar que no existen normas ni reglamentos que prohíban la expresión anónima o el uso de herramientas de cifrado que permite proteger la privacidad y seguridad de las comunicaciones.