Perú

¿Cuál es el marco legal que protege la privacidad? ¿Mis derechos están protegidos frente a la vigilancia estatal de las comunicaciones?

Perú está sujeto a tratados internacionales en materia de derechos humanos que ha ratificado. Estos tratados, como la Convención Interamericana de Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos, reconocen el derecho a la privacidad y otras libertades fundamentales. Dichos instrumentos son obligatorios y aplicables en el derecho interno.

El artículo 2 de la Constitución Política de 1993 protege el derecho de todos los ciudadanos a: (I) que los servicios informáticos no suministren informaciones que afecten la intimidad personal y familiar, (ii) a la intimidad personal y familiar, (iii) a la inviolabilidad del domicilio, y (iv) al secreto y a la inviolabilidad de sus comunicaciones y documentos privados. En esa línea, el Tribunal Constitucional peruano ha reconocido en repetida jurisprudencia los alcances de este derecho, que entiende como:

> *"[...] el ámbito personal en el cual un ser humano tiene la capacidad de desarrollar y fomentar libremente su personalidad. Por ende, se considera que está constituida por los datos, hechos o situaciones desconocidos para la comunidad que, siendo verídicos, están reservados al conocimiento del sujeto mismo y de un grupo reducido de personas, y cuya divulgación o conocimiento por otros trae aparejado algún daño".*[1]

En particular, el secreto de las comunicaciones también se encuentra protegido en el articulo 2 inciso 10 de la Constitución, que dice:

> 10. Al secreto y a la inviolabilidad de sus comunicaciones y documentos privados. Las comunicaciones, telecomunicaciones o sus instrumentos sólo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del Juez, con las garantías previstas en la ley. Se guarda secreto de los asuntos ajenos al hecho que motiva su examen.

También hay algunas normas legales que protegen el derecho a la privacidad y a la protección de datos personales. Entre ellas se encuentran:

1 Sentencia del Tribunal Constitucional recaída sobre el expediente No. 6712-2005-HC/TC. 17 de octubre de 2005.

- La ley de protección de datos personales indica en su articulo 13:

  "Las comunicaciones, telecomunicaciones, sistemas informáticos o sus instrumentos, cuando sean de carácter privado o uso privado, solo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez o con autorización de su titular, con las garantías previstas en la ley. Se guarda secreto de los asuntos ajenos al hecho que motiva su examen. Los datos personales obtenidos con violación de este precepto carecen de efecto legal".[2]

- El artículo 4 del Texto Único Ordenado de la Ley de Telecomunicaciones establece que la inviolabilidad y el secreto de las telecomunicaciones está protegido por la ley;

- El artículo 13 del Reglamento de Telecomunicaciones establece que una violación de este derecho se produce cuando alguien que no es ni el remitente ni destinatario roba deliberadamente, intercepta, interfiere, altera o cambia el texto de la comunicación, publica o lo usa en cualquier forma, o se desvía desde su curso previsto.

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

Para intervenir las comunicaciones - de cualquier manera - es necesario un procedimiento y este está descrito en la Ley 27.697 y detallado en los códigos Penal y Procesal Penal, así como en el Protocolo de Actuación Conjunta para la Intervención o Grabación de Registro de comunicaciones Telefónicas o de Otras Formas de Comunicación, aprobado por Resolución Ministerial No. 0243-2014-JUS.

Conforme a este marco legal, solo un juez puede autorizar a un fiscal hacer uso de la facultad de conocer y controlar las comunicaciones de las personas que son materia de investigación preliminar o jurisdiccional y solo si el hecho a investigar corresponde a una lista particular de delitos que abarcan los de:

> (i) secuestro, (ii) trata de personas, (iii) pornografía infantil, (iv) robo agravado, (v) extorsión, (vi) tráfico ilícito de drogas, (vii) tráfico ilícito de migrantes, (viii) delitos contra la humanidad, (ix) atentados contra la seguridad nacional y traición a la patria, (x) peculado, (xi) corrupción de funcionarios, (xii) terrorismo, (xiii) delitos tributarios y aduaneros, (xiv) lavado de activos, (xv) delitos informáticos.

¿Cómo pueden vigilar mis comunicaciones?

El procedimiento de intervención de las comunicaciones puede ser solicitado por los Fiscales Penales, los Procuradores Públicos y el Fiscal de la Nación exclusivamente y únicamente en los casos de su competencia. El proceso de vigilancia estatal de las comunicaciones es ejecutado por el personal autorizado del Ministerio Público y/o de la Policía Nacional del Perú bajo supervisión del fiscal a cargo de la investigación. Para ello, la ley señala que puede contar con el apoyo técnico de las empresas operadoras de comunicaciones a fin de asegurar la intervención o control de las mismas en tiempo real y, si las características de las comunicaciones lo requieren, también puede acudir a personas naturales o jurídicas expertas en la actividad de recolección. La solicitud que envíe el fiscal al juez debe de estar sustentada y contener todos los datos necesarios. Además, debe de especificar todos los factores e indicios que permitan al juez emitir la respectiva autorización de manera criteriosa. Si la solicitud es denegada, el fiscal puede apelar al superior jerárquico desde

2 Ley No. 29733, Ley de Protección de Datos Personales, disponible en: https://eff.org/r.beoh

el día siguiente de enterado o notificado. El pedido del fiscal y la autorización judicial deben de contener las especificaciones que sean necesarias para distinguir las distintas clases de recolección y de control que pretende llevarse a cabo, incluyendo:

1. Si la comunicación es una determinada; si se va a dar probablemente dentro de un conjunto indeterminado de comunicaciones; o si es una comunicación cierta que sucederá dentro de circunstancias determinadas.

2. Si la comunicación se dará en el futuro o ya se dio en el pasado.

3. Si la comunicación es accesible a toda persona que la perciba, a ella o su medio, o si se encuentra cerrada o cifrada.

4. Si se han hecho uso de medios destinados a encubrir la identidad del emisor o del receptor de la comunicación, o de cualquier otra persona, hecho o circunstancia que se mencionan en la comunicación; así como la puesta de cualquier dificultad destinada a impedir el acceso o la identificación de la comunicación, de sus partes, o de la información en ella mencionada.

El Sistema de Inteligencia Nacional también contempla situaciones en las que se puede recurrir a la vigilancia de las comunicaciones, según los procedimientos descritos en el Decreto Legislativo 1141 sobre el Fortalecimiento y Modernización del Sistema de Inteligencia Nacional - SINA y de la Dirección Nacional de Inteligencia – DINI y su reglamento.[3]

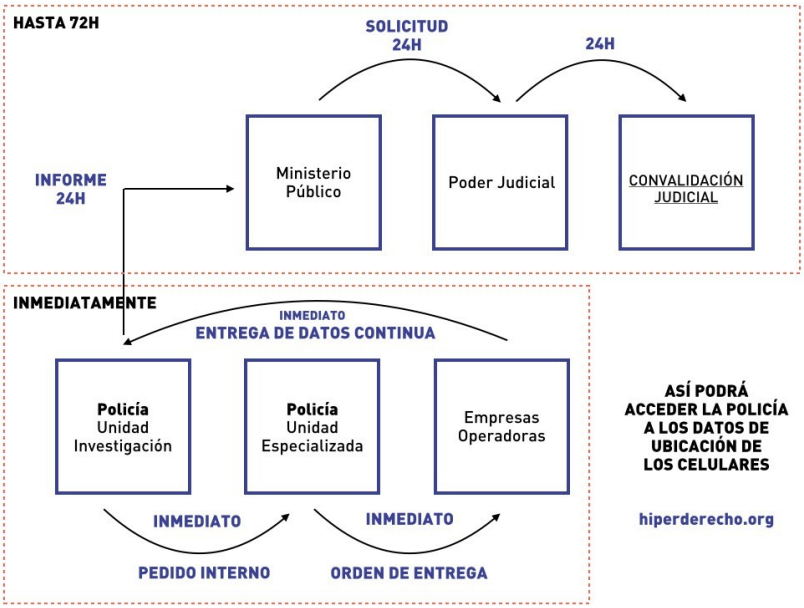
¿Están las empresas de telecomunicaciones obligadas a retener mis comunicaciones? ¿Bajo que condiciones la policía puede acceder a los datos de mi comunicación?

Si, el Decreto Legislativo No. 1182, vigente desde julio de 2015 obliga a las empresas de telecomunicaciones y las entidades públicas relacionadas con estos servicios deben conservar los datos derivados de las telecomunicaciones durante los primeros doce (12) meses en sistemas informáticos, y deben permitir su consulta y entrega en línea y en tiempo real previa orden judicial Concluido el referido periodo, deberán conservar dichos datos por veinticuatro (24) meses adicionales, en un sistema de almacenamiento electrónico.

La entrega de datos almacenados por un periodo no mayor a doce meses, se realiza en línea y en tiempo real después de recibida la autorización judicial. Para el caso de los datos almacenados por un periodo mayor a doce meses, se hará entrega dentro de los siete (7) días siguientes a la autorización judicial, bajo responsabilidad.

El decreto autoriza a la policía a requerir a cualquier empresa operadora de telecomunicaciones acceso a los datos de localización de teléfonos móviles o dispositivos electrónicos. Mayor información sobre la campana peruana contra el Decreto Legislativo 1182, aquí: http://www.hiperderecho.org/dl1182/

3 A inicios de febrero de 2015, mientras este informe se finalizaba, el Gobierno Peruano anunció su intención de reestructurar totalmente el Sistema de Inteligencia Nacional. Los resultados de esta reestructuración pueden implicar una renovación parcial o total de las normas legales reseñadas.



Según la norma, tras la solicitud de la policía, empresas de telecomunicaciones tales como Movistar o Claro están inmediatamente obligadas a proporcionar acceso en tiempo real previa solicitud simple, es decir, sin la necesidad de una autorización judicial previa. Este mecanismo procede cuando concurran tres requisitos en simultáneo: (i) se trate de un delito flagrante,[4] (ii) el delito investigado sea sancionado con pena superior a los cuatro años de cárcel, y, (iii) el acceso a esta información constituya un medio necesario para la investigación. El cumplimiento de estos requisitos solo será revisado luego de que la policía ya haya accedido a los datos. Así, la unidad a cargo de la investigación policial tendrá veinticuatro (24) horas para enviar al fiscal un informe que sustente su requerimiento y el fiscal tendrá otras veinticuatro (24) horas para solicitar a un juez la "convalidación [posterior] de la medida". A su vez, el juez que reciba el pedido tendrá otras 24 horas para pronunciarse sobre la legalidad del pedido y establecer un periodo durante la cual estará vigente.

En octubre de 2015, mediante Resolución Ministerial No. 0631-2015-IN, el Ministerio del Interior aprobó el "Protocolo de acceso a los datos de geolocalización de teléfonos móviles o dispositivos electrónicos de naturaleza similar", que establece las etapas del procedimiento de acceso a la información de geolocalización creado por el Decreto Legislativo No. 1182. Sin embargo, amparándose en la excepción de seguridad nacional de la Ley de Transparencia y Acceso a la Información Pública, el Ministerio ha considerado al texto mismo del Protocolo como de carácter "reservado".

¿Están protegidos mis datos de localización en la Constitución y la legislación Peruana?

Sí, la Constitución reconoce que toda persona tiene derecho al secreto y a la inviolabilidad de sus comunicaciones. En particular, señala que las comunicaciones, las telecomunicaciones y sus instrumentos solo pueden ser abiertos, incautados, interceptados o intervenidos por mandato motivado de un juez con las garantías previstas en la Ley. De igual forma, desde el año 2009 contamos con una norma especial aprobada por el Ministerio de Transportes y Comunicaciones que establece medidas destinadas a salvaguardar el derecho a la inviolabilidad y el secreto de las telecomunicaciones. Esta señala expresamente como parte del ámbito de protección del derecho al secreto e inviolabilidad de las telecomunicaciones "el origen, destino, realización, curso o duración de una comunicación.

¿Es legal usar cifrado?

No existe ninguna legislación o práctica que prohiba la utilización de cifrado.

4 Existe flagrancia cuando un delito se está cometiendo, se acaba de cometer y hasta 24 horas después de cometido (Código Procesal Penal 259)

¿Está el Estado autorizado a realizar ataques maliciosos para vigilar mis comunicaciones?

En el marco de una investigación penal, es posible que se ordene la interceptación de las comunicaciones telefónicas o de cualquier otra forma de comunicación (incluyendo las comunicaciones electrónicas). Además, también se admite la posibilidad de que mediante orden judicial se disponga la obtención de copias o respaldos de la correspondencia electrónica dirigida al imputado o emanada de él. A solicitud del Fiscal, también puede ordenarse judicialmente la incautación de bienes como computadoras y la exhibición forzosa de documentos privados para su conservación o copiado. Todas estas actividades son llevadas a cabo por el Ministerio Público con colaboración de la Policía Nacional. Sin embargo, no hay una mención expresa en el Código Procesal Penal para que se utilicen herramientas de vulneración de sistemas informáticos en la obtención de esta información, bajo la modalidad de "hackeo" remoto de computadoras y no se tiene conocimiento de que estos mecanismos vengan siendo usados formalmente.

¿Cómo me entero si el estado vigila mis comunicaciones?

El sujeto de la invención de las comunicaciones puede solicitar al juez - dentro de los tres días de la notificación - una reconsideración judicial. Sin embargo, el sistema de inteligencia mantendrá una reserva absoluta sobre lo actuado clasificando la información como secreta.

Pero si hablamos del acceso a los datos de geolocalización por parte de las autoridades, nos encontramos con que el usuario no será notificado, llegando al extremo de prohibir a las compañías operadores que revelen su participación en el espionaje al imposibilitarlos de revelar que información han compartido.

¿Cuántas comunicaciones han sido interceptadas por el Estado peruano?

La legislación peruana no obliga al estado peruano a ser transparente con sus actividades de vigilancia, como tampoco está sujeto al control público. Más allá de las notificaciones a las personas cuyas comunicaciones fueron investigadas como parte de una comunicación penal no vamos a encontrar mecanismos ni dispositivos legales que obliguen a las entidades que lleven a cabo estas actividades a informar sobre la cantidad de intervenciones, el tipo y el ámbito en que se han realizado.

En el caso del sistema de inteligencia, el único espacio de control que existe es la Comisión de Inteligencia del Congreso pero toda la información que le entrega también es clasificada como secreta.

Recientemente, la falta de control sobre las actividades del sistema de inteligencia motivó una crisis política que terminó con la desactivación del Sistema y su próxima reorganización.[5]

El estado peruano ha mostrado interés en proteger la privacidad de la población?

El Estado Peruano ha demostrado formalmente su compromiso con la privacidad aunque en los últimos años ha venido erosionando este derecho mediante la introducción de diversos dispositivos legales. En particular, algunas de las normas

5 Gobierno cerrará la DINI por 180 días para su reestructuración El Comercio, 9 de febrero de 2015, disponible en: https://eff.org/r.v79d

relacionadas con la seguridad ciudadana, la lucha contra el narcotráfico o la reforma del sistema de inteligencia han buscado eliminar las garantías legales para el acceso a información privada como comunicaciones o datos personales de los ciudadanos.

A partir de la entrada en vigencia del Decreto Legislativo Nro. 1182, la información que antes la policía sólo podía obtener mediante una autorización judicial expresa, ahora puede ser obtenida directamente de las empresas operadoras de telecomunicaciones a solo pedido si es que consideran que las personas vigiladas están dentro de las conductas punibles establecidas por el Decreto Legislativo en cuestión.