Contribución a la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos en relación con el Cuestionario de Consulta con motivo del Informe temático sobre el uso de las tecnologías de vigilancia digital en las Américas

Marco normativo y desafíos del uso de tecnologías de vigilancia digital en el Perú

1. Presentación de IDEHPUCP

El Instituto de Democracia y Derechos Humanos (IDEHPUCP) es una unidad académica de la Pontificia Universidad Católica del Perú creada en el 2004. A lo largo de sus 20 años de existencia, el IDEHPUCP ha abordado diversos retos relacionados con los derechos humanos y la democracia en el Perú y la región. En los últimos años, ha concentrado sus esfuerzos en comprender el impacto de las nuevas tecnologías en los derechos humanos. Desde 2022, se han organizado conversatorios, publicado informes sobre esta temática y proporcionado elementos técnicos de análisis jurídico para fortalecer el Proyecto de Reglamento de la Ley Nº 31814, que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país, desde un enfoque de derechos humanos. Aunado a ello, recientemente, el IDEHPUCP respondió a la convocatoria de aportes realizada por la experta independiente de Naciones Unidas en derechos humanos y solidaridad internacional, Cecilia M. Bailliet, brindándole información respecto al rol del Estado peruano en la promoción de la IA.

En línea con su compromiso continuo, el presente informe responde a la sección III del Cuestionario de Consulta sobre tecnologías de vigilancia digital y derechos humanos de la Comisión Interamericana de Derechos Humanos. Se examina la normativa peruana sobre vigilancia digital en el sistema penal y de inteligencia, así como en el marco de las investigaciones policiales. Finalmente, el informe presenta las conclusiones que buscan contribuir al debate sobre el equilibrio entre seguridad pública y protección de derechos fundamentales en la era digital.

2. Marco normativo peruano y vigilancia digital

El uso de tecnologías de vigilancia digital por parte del Estado peruano ha experimentado un crecimiento significativo en los últimos años, planteando importantes desafíos en términos de derechos humanos. Este informe examina el marco normativo que rige estas prácticas en Perú, abordando cuatro áreas críticas: la vigilancia en el sistema penal, el sistema de inteligencia, la geolocalización policial, y la colaboración de las empresas de telecomunicaciones. A través de este análisis, se busca proporcionar una visión integral de cómo el Estado peruano está equilibrando las necesidades de seguridad y aplicación de la ley con la protección de los derechos humanos en la era digital.

2.1. Vigilancia digital en el sistema penal peruano

El sistema penal peruano ha incorporado diversos mecanismos de vigilancia estatal, reflejando una tendencia hacia el uso de tecnologías digitales para el control y la

investigación criminal. Estos mecanismos se manifiestan principalmente en dos ámbitos: la vigilancia electrónica personal y la intervención de comunicaciones.

La vigilancia electrónica personal se introdujo como una medida de control mediante la Ley N°. 29499[1] y se reguló posteriormente a través del Decreto Legislativo N°. 1322[2]. Este mecanismo implica el uso de grilletes electrónicos para monitorear el desplazamiento de aquellas personas dentro de un radio definido judicialmente. Su objetivo principal es doble: servir como alternativa a las medidas de coerción procesal tradicionales y contribuir a la reducción del hacinamiento en los establecimientos penitenciarios. El Decreto Legislativo N°. 1514[3] ha introducido modificaciones adicionales al Código Penal y al Código Procesal Penal en esta materia, reforzando el marco legal de esta forma de vigilancia.

El Código Procesal Penal peruano, en sus artículos 207, 230 y 231, establece un marco detallado para la intervención de comunicaciones con fines de investigación y prevención del delito. Este marco incluye requisitos específicos para la intervención que exige autorización judicial previa, basada en elementos de convicción suficientes sobre la comisión de un delito grave (pena superior a cuatro años). La intervención puede abarcar comunicaciones telefónicas, radiales u otras formas de comunicación electrónica, con una duración inicial de hasta 60 días, prorrogables bajo justificación.

El procedimiento para la intervención de comunicaciones establece garantías importantes. Se requieren requisitos específicos para el requerimiento fiscal y la resolución judicial[4], incluyendo la identificación del afectado y los medios a intervenir. Además, se establecen protocolos rigurosos para el registro, grabación y custodia de la información obtenida, bajo la responsabilidad del fiscal. El Código también reconoce el derecho del afectado a ser notificado y a solicitar un reexamen judicial de la medida, aunque con ciertas limitaciones por razones de seguridad.

En casos de delitos graves como terrorismo, tráfico de drogas y secuestro, la ley prevé un mecanismo de emergencia que permite una intervención inmediata por parte del fiscal, sujeta a posterior convalidación judicial. Esta disposición busca equilibrar la necesidad de acción rápida en situaciones críticas con el requisito de supervisión judicial.

El artículo 207 del Código Procesal Penal autoriza, en casos de delitos graves o relacionados con el crimen organizado, la vigilancia mediante fotografías y otros medios técnicos de observación. Esta vigilancia puede ser ordenada directamente por el fiscal, excepto cuando se realiza en espacios privados, lo que requiere autorización judicial. Esta

---

[1] "Ley que establece la vigilancia electrónica personal e incorpora el artículo 29°A y modifica el artículo 52° del Código Penal, Decreto Legislativo Núm. 635; modifica los artículos 135° y 143° del Código Procesal Penal, Decreto Legislativo Núm. 638; y los artículos 50°, 52°, 55° y 56° del Código de Ejecución Penal, Decreto Legislativo Núm. 654". Publicada en el Diario Oficial El Peruano el 18 de enero de 2010.

[2] "Decreto Legislativo que regula la vigilancia electrónica personal". Publicado en el Diario Oficial El Peruano el 5 de enero de 2017.

[3] "Decreto legislativo que optimiza la aplicación de la medida de vigilancia electrónica personal como medida coercitiva personal y sanción penal a fin de reducir el hacinamiento". Publicado el 4 de junio de 2020.

[4] De acuerdo con el Artículo 230, numeral 3, del Nuevo Código Procesal Penal Peruano, tanto el requerimiento fiscal como la resolución judicial que autorice la intervención de comunicaciones deben especificar: el nombre y dirección del afectado (si se conocen), la identidad del medio de comunicación a intervenir (de ser posible), la forma, alcance y duración de la interceptación, y la dependencia policial o Fiscalía encargada de la diligencia. El juez debe comunicar al fiscal el mandato judicial de levantamiento del secreto de las comunicaciones, y la notificación a los concesionarios de servicios públicos de telecomunicaciones se realiza mediante oficio, transcribiendo la parte resolutiva pertinente para mantener la reserva del caso.

disposición amplía las herramientas de investigación disponibles para las autoridades, al tiempo que establece salvaguardas para la privacidad en espacios íntimos.

Complementando estas disposiciones, el Código Penal peruano tipifica una serie de delitos relacionados con la vigilancia ilegal por parte de actores privados. Estos incluyen la violación de la intimidad, el tráfico de datos personales, la interferencia telefónica y la violación del secreto de las comunicaciones, entre otros. Al respecto, se debe destacar la labor del Tribunal Constitucional peruano en desarrollar estándares jurisprudenciales sobre el uso de drones y cámaras de video vigilancia a fin de garantizar el derecho a la vida privada, mediante sentencia Nº 411-2020-HC/TC. En relación al uso de drones por agentes privados determinó siete criterios para establecer estándares de privacidad sobre su uso, entre los que destacamos: i) la intrusión de drones debe ser justificada, razonable y proporcional al beneficio que pretende obtener; ii) los operadores de drones tienen prohibido sobrevolar los predios privados o del Estado sin autorización previa del morador o autoridad pertinente, salvo situaciones de interés público y de carácter humanitario; iii) la recopilación de datos personales mediante el uso de drones sería ilícita en los casos en que se realice dentro de un predio de uso propio, o cuando se actúe dentro de su perímetro sin invadir el espacio público o de terceros y iv) la necesidad de prohibirse el sobrevuelo de drones sobre aglomeraciones de personas incluso estando en espacios públicos.

Ante ello, el Estado fortaleció esta tipificación para proteger los derechos de las personas frente a posibles abusos en el ámbito privado. No obstante, la preocupación por un marco regulatorio específico para la vigilancia digital, en el contexto emergente de nuevas tecnologías es aún inexistente en el país. A pesar de contar con esfuerzos desde el Estado para regular el uso de la Inteligencia Artificial[5] y sus implicancias en el ámbito de la vigilancia, aún no se cuenta con el desarrollo reglamentario respectivo[6] .

2.2. Vigilancia digital por parte del Sistema de Inteligencia Nacional

El Sistema de Inteligencia Nacional (SINA) es el conjunto de relaciones funcionales entre los organismos de inteligencia del Estado peruano, con el objetivo de generar conocimiento útil para la toma de decisiones en seguridad nacional, proteger las capacidades nacionales frente a amenazas externas y asegurar la seguridad digital en este ámbito[7]. De acuerdo con el Decreto Legislativo 1141[8], el SINA contempla situaciones en las que puede recurrir a la vigilancia de las comunicaciones. Con ello, el Estado cuenta con facultades legales para la vigilancia social, bajo el cumplimiento de los objetivos de la institución y la Dirección Nacional de Inteligencia (DINI).

El Decreto Legislativo 1141 regula los procedimientos especiales de obtención de información y vigilancia, los cuales requieren autorización de jueces superiores ad hoc designados por la Corte Suprema. Estas solicitudes, realizadas exclusivamente por el Director de la DINI, deben detallar la identificación de los afectados, las medidas solicitadas, y su duración. No obstante, existen situaciones de urgencia donde el Director puede

[5] Para mayor detalle: https://cdn.www.gob.pe/uploads/document/file/5038703/ley-que-promueve-el-uso-de-la-inteligencia-artificial-en-fav-ley-n-31814.pdf?v=1692895308

[6] Para mayor información: https://idehpucp.pucp.edu.pe/publicaciones/comentarios-generales-al-proyecto-de-decreto-supremo-que-aprueba-el-reglamento-de-la-ley-no-31814-ley-que-promueve-el-uso-de-la-inteligencia-artificial-en-favor-del-desarrollo-economico-y-social-del/

[7] Para mayor información: https://www.gob.pe/27632-sistema-de-inteligencia-nacional-sina

[8] Decreto legislativo de fortalecimiento y modernización del Sistema de Inteligencia Nacional - SINA y de la Dirección Nacional de Inteligencia - DINI

autorizar procedimientos sin aprobación judicial previa, comprometiéndose a formalizar su solicitud ante el Juez Superior Ad hoc en un plazo de 24 horas.

Asimismo, cabe resaltar que la DINI no es ajena a la posibilidad del control externo en el marco de sus actividades de vigilancia sobre el sistema de inteligencia. El Congreso de la República, el Poder Judicial, la Contraloría General de la República y el Defensor del Pueblo, de acuerdo con el artículo 5 del Decretp Legislativo 1141, pueden solicitar acceso a la información clasificada de inteligencia del SINA, la cual debe ser proporcionada de forma obligatoria por la DINI. De igual manera, de acuerdo con el artículo 25 de la norma, el Director de Inteligencia Nacional y el Director Ejecutivo de la DINI se encuentran sometidos al control e investigaciones por parte del Poder Ejecutivo, Legislativo, Judicial, Ministerio Público y Contraloría General de la República.

Los informes de inteligencia no tienen ningún valor probatorio dentro de los procesos judiciales, administrativos y disciplinarios, pero su contenido podrá constituir elemento orientador de la investigación. Sin embargo, según el artículo 35, la información obtenida de las intervenciones de vigilancia, que sea innecesaria para el objetivo del sistema por corresponder a los derechos fundamentales y la vida privada de la persona, debe ser destruida por los funcionarios responsables, bajo responsabilidad de inhabilitación y sin perjuicio de sanciones correspondientes.

Cabe resaltar que el SINA, en su esquema organizacional, según el artículo 9, se encuentra conformado en dos niveles por altos cargos de las Fuerzas Armadas y del Ministerio del Interior. En los Órganos de Inteligencia del Sector Defensa, se encuentra la Segunda División del Estado Mayor Conjunto de las Fuerzas Armadas, la Dirección de Inteligencia del Ejército del Perú, la Dirección de Inteligencia de la Marina de Guerra del Perú y la Dirección de Inteligencia de la Fuerza Aérea del Perú.

Por su lado, en los Órganos de Inteligencia del Sector Interior, se encuentra la Dirección General de Inteligencia del Ministerio del Interior y la Dirección de Inteligencia de la Policía Nacional del Perú. Con ello, las fuerzas del orden tienen un rol predominante en el acceso a herramientas de vigilancia y control de la información, lo cual, en el presente escenario de debilitamiento del estado de derecho[9], se podría correr el riesgo de un mal uso de los sistemas de inteligencia para satisfacer intereses personales o ejercer presión contra la sociedad civil.

No obstante, su función institucional en el uso de la vigilancia del sistema de inteligencia reside en el enfrentamiento y detección de “nuevas amenazas” a la seguridad, sea de carácter intra o extraestatal[10]. Sin embargo, el clima político nacional, caracterizado por la criminalización de la protesta y el uso del aparato represivo del Estado contra los civiles, la posibilidad de utilizar estos servicios en situaciones de “urgencia”, sin necesitar de una autorización en el momento por parte de un juez, puede terminar en serias situaciones que transgredan el pleno ejercicio de derechos humanos de determinadas personas o grupos son vigilados por ser supuestas “amenazas”[11].

---

[9] Para mayor detalle revisar Barrenechea, R. y Vergara, A. (2024). Democracia Asaltada. El colapso de la política peruana (y una advertencia para América Latina). Fondo Editorial de la Universidad del Pacífico.
[10] Arce, G. (s/f). El rol del sistema de inteligencia en un régimen democrático. Desco.https://www.desco.org.pe/recursos/sites/indice/752/2105.pdf

[11] Para detalles de la situación de la protesta en Perú, revisar: https://www.elsaltodiario.com/peru/criminalizacion-persecucion-dirigentes-protesta-ayacucho-castillo-fiscalia

2.3. Vigilancia digital por parte de la Policía Nacional del Perú

El Decreto Legislativo N° 1182[12] representa una grave amenaza para los derechos humanos y las libertades fundamentales en el país. Esta norma, que permite a la Policía Nacional del Perú (PNP) acceder a los datos de geolocalización en tiempo real de cualquier usuario de dispositivos móviles o electrónicos, socava seriamente el derecho a la privacidad y establece un peligroso precedente de vigilancia estatal sin las debidas garantías judiciales.

Según el análisis realizado por Hiperderecho, este decreto crea un mecanismo mediante el cual la PNP puede solicitar directamente a las empresas de telecomunicaciones el acceso inmediato a los datos de localización o geolocalización de teléfonos móviles o dispositivos electrónicos, sin necesidad de una autorización judicial previa[13]. Esto representa una clara violación al debido proceso y al principio de reserva judicial, que tradicionalmente ha sido un salvaguarda fundamental contra el abuso de poder por parte de las autoridades.

El decreto establece que la PNP puede utilizar este mecanismo en casos de flagrante delito, cuando el delito investigado sea sancionado con pena superior a cuatro años de cárcel, y cuando el acceso a esta información sea necesario para la investigación. Sin embargo, conforme al artículo 5.1, la verificación de estos requisitos sólo se realiza después de que la policía ya ha accedido a los datos, lo que abre la puerta a posibles abusos y violaciones de derechos.

Más preocupante aún es el hecho de que, bajo este nuevo sistema, pueden transcurrir hasta 72 horas desde que la PNP comienza a monitorear a una personas hasta que un juez se pronuncie sobre la legalidad de la medida. Durante este tiempo, la privacidad y los derechos de la persona intervenida quedan completamente desprotegidos, sin ningún tipo de supervisión judicial efectiva.

Otro aspecto alarmante del Decreto Legislativo N° 1182 es la falta de transparencia en su implementación. El Ministerio del Interior ha clasificado como "reservado" el protocolo que establece las etapas del procedimiento de acceso a la información de geolocalización, amparándose en la excepción de seguridad nacional de la Ley de Transparencia y Acceso a la Información Pública. Esto significa que la población en general no puede conocer los detalles de cómo se está aplicando una medida que potencialmente viola sus derechos humanos.

Conclusiones

A lo largo del desarrollo del presente informe ha quedado demostrada la complejidad y los desafíos que enfrentan los derechos humanos en el contexto del uso creciente de tecnologías de vigilancia en el Perú. Asimismo, se ha hecho énfasis en la necesidad de equilibrar las demandas de seguridad nacional con la protección de los derechos humanos, especialmente en un entorno digital donde las herramientas de vigilancia se han vuelto más sofisticadas y accesibles para el Estado. Por ello, es crucial mantener una vigilancia

---

[12]"Decreto legislativo que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado". Publicado en el Diario Oficial El Peruano el 5 de enero de 2017.

[13] Croci, G. (2017, 14 de septiembre). *Vigilancia estatal y transparencia en Perú.* Hiperderecho. https://hiperderecho.org/2017/09/vigilancia-estatal-transparencia-peru/

constante por parte de la sociedad civil y las instituciones de derechos humanos para asegurar que estas herramientas de vigilancia se utilicen de manera proporcional y respetando el Estado de Derecho.

El sistema penal peruano, el uso de tecnologías como la vigilancia electrónica y la intervención de comunicaciones ha mostrado ser un mecanismo útil para el control del crimen y la reducción del hacinamiento penitenciario. Sin embargo, estas medidas también plantean desafíos significativos para la privacidad y derechos de las personas, lo que subraya la necesidad de contar con salvaguardias legales adecuadas y una supervisión judicial estricta para prevenir posibles abusos. Asimismo, se ha analizado el papel del SINA, donde se evidencia una preocupación por el potencial uso indebido de las herramientas de vigilancia por parte de las fuerzas de seguridad. La estructura y las facultades de estos organismos, en un contexto de crisis política y criminalización de la protesta que se vive actualmente, plantean el riesgo de que se utilicen estas tecnologías contra las personas que no representan una amenaza real, lo que podría erosionar aún más los derechos humanos en el país.

Por otro lado, el Decreto Legislativo N°. 1182 representa un retroceso significativo en la protección de los derechos humanos en Perú. Aunque se presenta como una herramienta para combatir la delincuencia y el crimen organizado, en realidad establece un sistema de vigilancia masiva por parte de la Policía Nacional que, en colaboración con las empresas de telecomunicaciones, puede acceder a los datos de localización y geolocalización de una persona en tiempo real y sin autorización judicial, con escasas salvaguardas legales. Es imperativo que se revise y modifique esta ley para garantizar un equilibrio adecuado entre la seguridad pública y el respeto a los derechos humanos de la población. Asimismo urge fortalecer las garantías legales para evitar abusos y asegurar que estas medidas se estén aplicando de manera proporcional y justa.

En suma, el informe pone de manifiesto la urgente necesidad de un enfoque equilibrado y cuidadoso en la implementación de tecnologías de vigilancia en el Perú. Aunque estas herramientas pueden contribuir a la seguridad pública, su uso indiscriminado y sin las garantías necesarias puede socavar los derechos humanos de las personas. Es esencial que las autoridades peruanas revisen y refuercen el marco legal existente para garantizar que las prácticas de vigilancia respeten plenamente los derechos humanos, al mismo tiempo que promueven un entorno seguro para la población.