VIGILADOS EN SECRETO

normas, prácticas y silencios

en el acceso a información pública sobre vigilancia

LUCÍA LEÓN PACHECO

HIPER DERE CHO
Tecnología como libertad

Vigilados en secreto: normas, prácticas y silencios en el acceso a información pública sobre vigilancia

Vigilados en secreto es una publicación realizada en el marco del proyecto "Desvelando las prácticas de vigilancia en el Perú", desarrollado por la asociación civil Hiperderecho entre 2024 y 2025.

Financiamiento
Agradecemos a *Rights & Security International* por financiar esta investigación.

Autoría
Lucía León Pacheco

Revisión legal
Dilmar Villena
Rubiela Gaspar Clavo

Diagramación
Lucía León Pacheco

Ilustraciones de portada e interiores
Jugo gástrico

Diagramación de portada
Lorena Marks

Asociación Civil Hiperderecho
hola@hiperderecho.org

Algunos derechos reservados, agosto de 2025
Bajo una licencia Creative Commons Reconocimiento 4.0 Internacional (CC BY 4.0).
Usted puede copiar, distribuir o modificar esta obra sin permiso de sus autoras siempre que reconozca su autoría original. Para ver una copia de esta licencia, visite:
https://creativecommons.org/licenses/by/4.0/deed.es

CONTENIDOS

INTRODUCCIÓN: VIGILADOS EN SECRETO

El derecho a la privacidad y el acceso a la información pública son pilares fundamentales en una sociedad democrática. En el Perú, sin embargo, esta relación enfrenta tensiones crecientes. Aunque las más evidentes se refieren a la publicidad de información que pertenece a la esfera privada de las personas, hay otras tensiones mucho menos visibles que merecen una particular atención por la gravedad que revisten. Este es el caso de la falta de transparencia sobre las acciones de gobierno que habilitan, posibilitan y promueven un estado general de vigilancia sobre la ciudadanía.

A pesar de que la Constitución reconoce el derecho al secreto de las comunicaciones y establece que su levantamiento solo puede realizarse mediante orden judicial, el marco normativo ha habilitado excepciones que, en la práctica, erosionan esas garantías. Leyes, reglamentos y prácticas institucionales han ampliado las facultades de entidades públicas para vigilar a la ciudadanía sin una supervisión suficiente y sin los controles adecuados.

Para poder dar cuenta de esta problemática, en el primer capítulo se ofrece un marco general sobre la vigilancia gubernamental y sus principales manifestaciones en relación con las tecnologías. Además, se explica cómo y

por qué estas prácticas colisionan con ciertos derechos fundamentales.

El segundo capítulo examina cómo diversos órganos del Estado —desde la Policía Nacional del Perú hasta el ente regulador de las telecomunicaciones (OSIPTEL)— han acumulado facultades para llevar a cabo acciones de vigilancia con una creciente opacidad. Muchas de estas facultades se justifican bajo conceptos amplios como "seguridad nacional", lo que no solo les permite ejercer vigilancia sin salvaguardias apropiadas, sino también restringe el escrutinio público sobre su funcionamiento.

Con el propósito de entender en qué medida la opacidad alrededor de la vigilancia tiene un amparo legal, el tercer capítulo se centra en la normativa de transparencia, sus excepciones y los estándares actuales para su interpretación. Además, se toma nota de las disposiciones sobre transparencia paralelas en materia de inteligencia.

Finalmente, el cuarto capítulo da cuenta de cómo se emplea la cláusula de seguridad nacional y el marco de excepciones al derecho de acceso a la información pública en la práctica. Así, luego de reflexionar críticamente sobre el rol actual que se le da al concepto de "seguridad nacional", se ofrecen los hallazgos principales de casos concretos de opacidad estudiados por Hiperderecho.

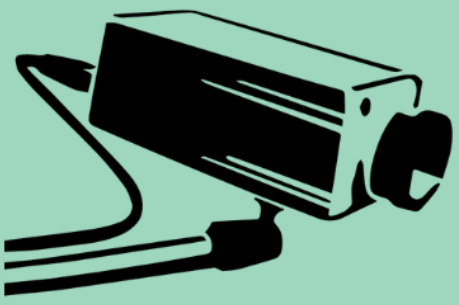
Este informe sostiene que la vigilancia estatal en el Perú se ejerce en condiciones de escasa transparencia, y que el propio marco legal habilita zonas exentas de control bajo el argumento de la seguridad nacional. Analizando normas, respuestas institucionales a solicitudes de acceso a la información, y las formas en que se aplica —o niega— la transparencia en estos casos, buscamos *demostrar el papel dual que juega la cláusula de seguridad nacional en este contexto:* por un lado, amplía el margen de acción de entidades estatales para vigilar; por otro, bloquea el control ciudadano sobre dichas acciones.

Frente a ello, urge abrir el debate sobre qué se entiende por seguridad nacional y cómo se decide qué información puede mantenerse reservada. Si los marcos de vigilancia y las excepciones a la transparencia no son revisados con mirada crítica, se naturalizan prácticas que debilitan los derechos fundamentales, desalientan la participación ciudadana y generan un clima de autocensura. Este informe busca contribuir a esa discusión, y ofrecer insumos para avanzar hacia un equilibrio más justo entre seguridad, transparencia y derechos humanos.

CAPÍTULO 1: MARCO GENERAL DE LA VIGILANCIA

1. ¿QUÉ ES LA VIGILANCIA?

No es una sorpresa que el desarrollo tecnológico supone un desafío particular para la privacidad. Este fue el caso, por ejemplo, de la fotografía instantánea, que motivó la publicación del clásico "The Right to Privacy" de Warren y Brandeis en 1890: en él, se propone la defensa del derecho a la privacidad (o a ser *dejado en paz*), frente a la forma en que la fotografía instantánea y la industria mediática estaban "invadiendo los recintos sagrados de la vida privada y familiar"[1].



Sin embargo, la velocidad de la innovación y los nuevos tipos de tecnología disponible sí nos enfrentan a retos mucho más complejos en términos de privacidad. La cada vez más veloz evolución de las capacidades tecnológicas de los gobiernos y empresas en el siglo XXI les permite, precisamente, mayores posibilidades para interceptar, extraer, filtrar, almacenar, analizar y difundir las comunicaciones privadas de comunidades enteras[2].

Este nuevo contexto responde no solo a ca-

1 Samuel D. Warren y Louis D. Brandeis (1980). *"The Right to Privacy"*, 4 Harvard Law Review 193.

2 Privacy International (2021), "PI's Guide to International Law and Surveillance". Disponible en: https://privacyinternational.org/sites/default/files/2022-01/2021%20GILS%20version%203.0_0.pdf

pacidades "mejoradas", sino a condiciones más favorables para la vigilancia. Nuestra huella digital, los metadatos, las copias de seguridad, el aprendizaje automático, el Internet de las cosas, entre otros, son componentes que, junto con una capacidad potenciada para procesar y cruzar mayores volúmenes de datos, permiten monitorear más fácilmente las actividades de las personas (desde la ubicación hasta el nivel de batería de un dispositivo). Esta ingente cantidad de información, además de ser recopilada y procesada con mayor facilidad, se almacena a costos mucho menores[3].

Estas condiciones tecnológicas, en combinación con el marco legal —muchas veces, opaco—, habilitan lo que denominamos **vigilancia estatal:** aquellas actividades de monitoreo, interceptación, recolección, análisis, uso, preservación y retención de información sobre las actividades, comunicaciones y datos[4] de personas o colectividades por parte de entidades gubernamentales o agentes estatales[5]. Para ello, el Estado despliega mecanismos de vigilancia que pueden ser masivos —es decir, que recogen información a gran escala— o dirigidos hacia personas específicas bajo monitoreo particular[6].

Para ello, los distintos agentes gubernamentales emplean diversas técnicas o aprovechan múltiples tipos de tecnologías. Algunos de los mecanismos más comunes documentados son los siguientes:

- **Intervención de las comunicaciones**: Consiste en el acceso, escucha o interceptación de comunicaciones privadas

---

3 Consejo de Derechos Humanos (2014). Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos: "El derecho a la privacidad en la era digital". Resolución A/HRC/27/37.

4 Necessary and Proportionate Principles (2014). International principles on the application of human rights to communications surveillance, p. 4. Disponible en: https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf

5 Aunque la vigilancia también es perfectamente posible por parte de empresas —y, de hecho, se realiza con fines comerciales—, este informe está centrado en la vigilancia por parte del Estado. Este tipo de vigilancia puede involucrar, en ocasiones, al sector privado, como se verá en las próximas secciones.

6 Access Now (2022). "Navigating the surveillance technology ecosystem", p. 6. Disponible en: https://www.accessnow.org/wp-content/uploads/2022/03/2022_STAP_Guide.pdf

(por ejemplo, llamadas telefónicas o correos electrónicos). Esto no solo involucra el contenido de la comunicación, sino también los metadatos asociados, que incluyen información sobre el tiempo, lugar, duración, patrones de comunicación y actividad en línea. Este proceso permite a las autoridades recopilar datos que, aunque aparentemente inconexos, pueden ser analizados para formar perfiles completos de individuos o grupos. Generalmente, los países —incluyendo Perú— cuentan con un marco legal detallado sobre las situaciones que habilitan este tipo de prácticas, así como los requisitos que deben cumplirse.

- **Geolocalización**: Es un proceso que permite identificar la ubicación geográfica de un dispositivo o persona, con distintos niveles de precisión. Puede realizarse en tiempo real o involucrar información sistematizada del pasado. La geolocalización revela información importante sobre una persona, incluyendo patrones de comportamiento, desplazamientos frecuentes y sus consiguientes correlaciones con actividades religiosas, políticas, de salud, entre otras.
- **Monitoreo de actividad en redes sociales**: Se refiere a la vigilancia sistemática o selectiva de las interacciones, publicaciones, comentarios, contactos y otros comportamientos de usuarios en plataformas como Facebook, X (antes Twitter), TikTok, Instagram, etc. Esta práctica puede incluir desde el análisis manual de contenidos hasta el uso de herramientas automatizadas para rastrear tendencias, identificar perfiles específicos o recolectar datos en masa.
- **Videovigilancia**: Es una tecnología que utiliza cámaras —generalmente, de circuito cerrado o CCTV— para registrar de forma continua o intermitente lo que ocurre en espacios determinados. Esta forma de vigilancia puede ser realizada en tiempo real o en diferido. Asimismo, su despliegue incluye la planificación de distribución y ubicación de estas cámaras en zonas estratégicas[7]. Cuando no se diseña apro-

[7] Carlos Guerrero (2019). "Videovigilancia urbana". Disponible en: https://hiperderecho.org/2019/05/videovigilancia-urbana/

piadamente su uso, pueden crear una falsa sensación de seguridad, mientras facilitan prácticas intrusivas o, incluso, discriminatorias[8].

- **Reconocimiento biométrico:** Se trata de tecnologías que analizan características físicas o de comportamiento únicas de una persona —como huellas dactilares, rasgos faciales, voz, forma de caminar o incluso patrones de emociones— para verificar, identificar o clasificar identidades. Aunque puede emplearse para autenticar identidades —como en el desbloqueo de dispositivos móviles—, también se utiliza para identificar personas, ya sea contrastando con bases de datos que incluyen específicos que contienen sus datos o con repositorios abiertos[9]. Su implementación, especialmente en contextos de seguridad pública, permite identificar individuos de manera remota y automatizada, incluso en tiempo real. Estas tecnologías representan un salto en la capacidad estatal de vigilancia, pasando del monitoreo de actividades a la identificación individual a gran escala.
- **Software espía (*spyware*)**: Es un tipo de software malicioso que se instala en un dispositivo sin que el usuario lo sepa y que recolecta información sin su consentimiento. Generalmente, está diseñado para acceder a mensajes, llamadas, correos electrónicos, archivos, historial de navegación, ubicación e incluso activar el micrófono o la cámara del dispositivo comprometido. Se trata de una herramienta altamente intrusiva, especialmente en sus versiones más avanzadas, que operan sin dejar rastros visibles y resultan prácticamente indetectables.

  El caso más emblemático de *spyware* es *Pegasus*, un sistema comercializado por la empresa israelí NSO Group y vendido

---

8 European Data Protection Supervisor (s/a). "Video-surveillance". Disponible en: https://www.edps.europa.eu/data-protection/data-protection/reference-library/video-surveillance_en

9 European Union Agency for Fundamental Rights (2019), Facial recognition technology: fundamental rights considerations in the context of law enforcement, p. 7. Disponible en: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

a gobiernos: sus clientes incluyen más de 60 agencias gubernamentales en 45 países[10].

Generalmente, estos y otros mecanismos de vigilancia se sostienen sobre argumentos que apelan a la seguridad nacional, la prevención del delito, la lucha contra el terrorismo o la protección del orden público. Así, las formas de monitoreo se presentan como actividades de interés público que habilitan la limitación de derechos fundamentales. No obstante, muchas veces no se realizan respetando mecanismos de control adecuados ni garantías judiciales, lo que da lugar al abuso y la afectación desproporcionada de derechos.

2. DERECHOS EN TENSIÓN

El despliegue de estas actividades de vigilancia estatal —ya sea mediante tecnologías como el reconocimiento biométrico, el spyware o el monitoreo de redes sociales— impacta de manera transversal en múltiples derechos fundamentales. Cuando las personas saben o sospechan que son vigiladas, pueden limitar sus desplazamientos, evitar participar en reuniones o abstenerse de expresar opiniones críticas, lo que erosiona libertades básicas como la de asociación, movimiento o expresión. Bajo marcos legales ambiguos o con escasa supervisión, se intensifica un escenario de alta vulnerabilidad para la ciudadanía. En este análisis, nos centraremos en dos dimensiones particularmente críticas: la privacidad (desde una concepción amplia) y la libertad de expresión.

2.1. Derecho a la privacidad

Por definición, la vigilancia impacta directamente en el derecho a la privacidad de las personas, quienes son monitoreadas sin su consentimiento y, la mayoría del tiempo, sin saberlo. En contraste, lo que garantiza este derecho es que la información relacionada

[10] Consejo de Derechos Humanos (2022). Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos: "El derecho a la privacidad en la era digital", párr. 6 y ss. A/HRC/51/17.

con la intimidad personal familiar de alguien no sea objeto de acceso, registro o alteración por parte de terceros sin que exista una autorización previa.

Así, la Declaración Universal de Derechos Humanos señala que nadie puede ser objeto de injerencias *arbitrarias o ilegítimas* a su vida privada, familia, domicilio o correspondencia, frente a lo cual debe haber una protección legal[11], criterio que también está presente en la Convención Americana sobre Derechos Humanos[12] y en el Pacto Internacional de Derechos Civiles y Políticos[13] (ambos vinculantes para el Perú). Como se advierte, el marco internacional desliza la idea de que sí existen formas legales de realizar este tipo de acciones, para lo cual existen una serie de estándares: principio de legalidad, objetivo legítimo, idoneidad, necesidad, proporcionalidad, autoridad judicial competente, debido proceso, derecho al recurso, notificación al usuario, entre otros.

En el marco constitucional peruano, el Tribunal Constitucional ha reconocido diversas manifestaciones vinculadas con lo que aquí llamamos "privacidad", las que considera derechos autónomos. Para efectos de este análisis, agruparemos estas garantías bajo la categoría amplia de "privacidad", entendida como un derecho compuesto que integra dichas dimensiones. Este acercamiento metodológico busca dar una visión práctica y accesible, sin perder de vista que cada una de estas facetas tiene un reconocimiento propio en la jurisprudencia constitucional.

La Constitución se refiere en más de una ocasión a distintas esferas de la vida privada que ameritan una protección particular. Así, en el artículo 2, el cual consagra los derechos fundamentales sin realizar una lista cerrada, se reconoce que toda persona tiene derecho (i) a que los servicios informáticos no suministren informaciones que afecten su intimidad personal y familiar[14]; (ii) a la intimidad personal y familiar[15]; (iii) a la inviolabilidad de su domicilio[16]; (iv) al

[11] Artículo 12, DUDH.

[12] Artículo 11, CADH.

[13] Artículo 17, PICDP.

[14] Artículo 2.6 de la Constitución Política del Perú.

[15] Artículo 2.7 de la Constitución Política del Perú.

[16] Artículo 2.9 de la Constitución Política del Perú.

secreto y a la inviolabilidad de sus comunicaciones y documentos privados, los que solo pueden ser intervenidos por mandato judicial motivado[17]; y (v) a mantener reserva sobre sus convicciones (políticas, filosóficas, religiosas o de cualquiera otra índole)[18].

Además, algunas de estas disposiciones constitucionales tienen un desarrollo en legislación específica. Así, por ejemplo, el Tribunal Constitucional ha considerado que el derecho "a que los servicios informáticos no suministren informaciones que afecten [la] intimidad personal y familiar" de las personas, consagrado en el artículo 2.6 de la Constitución, es la base del derecho a la autodeterminación informativa[19], cuyo desarrollo legal corresponde a la Ley de Protección de Datos Personales y su Reglamento.

Estas normas hacen énfasis en que el tratamiento de datos solo puede realizarse con consentimiento de su titular, siguiendo principios como la proporcionalidad, legalidad y finalidad lícita. Además, la Ley enfatiza —siguiendo el precepto constitucional— que las comunicaciones, sistemas informáticos o sus instrumentos, cuando sean de naturaleza privada, solo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento judicial motivado o con autorización de su titular, respetando las garantías previstas en la ley[20]. La normativa en materia de telecomunicaciones, por su parte, también hace énfasis en este derecho, estableciendo que los concesionarios de concesionarios de telecomunicaciones están obligados a salvaguardar el secreto de las telecomunicaciones y la protección de datos personales y adoptar medidas para garantizar la inviolabilidad y el secreto de las comunicaciones cursadas a través de tales servicios[21].

En adición, la "Norma que establece medidas destinadas a salvaguardar el derecho a la inviolabilidad y el secreto de las telecomunicaciones y la protección de datos personales, y regula las acciones de supervisión y control a cargo del Ministerio de Transportes y Comunicaciones" (aprobada por Resolución Ministerial Nº 111-

17 Artículo 2.10 de la Constitución Política del Perú.

18 Artículo 2.18 de la Constitución Política del Perú.

19 Sentencias recaídas en los expedientes 01797-2002-PHD/TC y 04387-2011-PHD/TC.

20 Artículo 13.4 de la Ley 29733, Ley de Protección de Datos Personales.

21 Artículo 13 del TUO de la Ley de Telecomunicaciones.

2009-MTC-03), delimita de manera mucho más específica el ámbito de protección del derecho a la inviolabilidad, secreto de las comunicaciones y protección de datos personales en el sector. En este caso, dicha protección alcanza a:

- El contenido completo de las comunicaciones de voz o datos transmitidas mediante redes de telecomunicaciones u otros medios tecnológicos disponibles.
- Los mensajes de texto y multimedia (como SMS y MMS), tanto los que se envían como los que se reciben.
- Los datos que revelan el origen, destino, duración, curso o realización de una comunicación.
- La información generada por el tráfico de comunicaciones de usuarios o abonados.
- Los registros codificados y decodificados asociados a llamadas realizadas.
- Documentos físicos, magnéticos o bases de datos que almacenen información relacionada con las comunicaciones, incluyendo los vinculados a servicios de televisión por cable o acceso a Internet.
- Los datos personales que las empresas operadoras recopilan de sus clientes durante su actividad comercial, siempre que no exista autorización expresa para su uso o una habilitación legal vigente.
- La información vinculada a pagos por servicios, como adelantos, pagos en cuotas o notificaciones de deuda.
- Los motivos específicos de suspensión del servicio, cuando esta no se deba al incumplimiento de pago, así como los datos sobre la reconexión o desconexión del mismo.

2.2. Libertad de expresión

Además de afectar la privacidad, la vigilancia estatal también tiene impactos directos sobre la libertad de expresión, uno de los pilares fundamentales de toda sociedad democrática. Uno de sus principales efectos —ya sea que exista certeza de ser vigilado o simplemente

temor a ello— es la generación de un efecto inhibidor: la sola posibilidad de estar bajo vigilancia puede llevar a una persona a restringir la manifestación de sus opiniones por miedo a represalias.

Este fenómeno de autocensura se produce, precisamente, por el temor a eventuales sanciones, incluso cuando estas estén dirigidas a un tipo específico de discurso. La incertidumbre sobre los límites de lo que podría considerarse problemático puede llevar a las personas a guardar silencio[22], limitando así el ejercicio pleno de su derecho a expresarse libremente. Este efecto inhibidor ha sido ampliamente documentado: investigaciones han demostrado que distintos tipos de vigilancia en línea reducen la participación y expresión digital, incluso de forma indirecta, cuando personas del entorno de la persona—como contactos en redes sociales— son objeto de procesos legales, hostigamiento o posible vigilancia estatal[23].

Mención particular merece la vigilancia contra personas defensoras de derechos humanos y periodistas, ya que socava las posibilidades de contar con una prensa libre, independiente y segura. Se trata de un grupo especialmente vulnerable y expuesto, no solo por la información que manejan, sino por el rol que cumplen: precisamente en contextos autoritarios o regresivos, los gobiernos buscan suprimir la disidencia política, la supervisión de la sociedad civil y la defensa de derechos fundamentales. Así, por ejemplo, en 2022 un peritaje técnico de Access Now y Citizen Lab identificó que al menos 35 personas de la sociedad civil y el periodismo salvadoreño —22 de ellas del medio *El Faro*— habían sido objeto de espionaje mediante el spyware Pegasus, lo que motivó un pronunciamiento formal por parte de la Comisión Interamericana de Derechos Humanos (CIDH)[24].

---

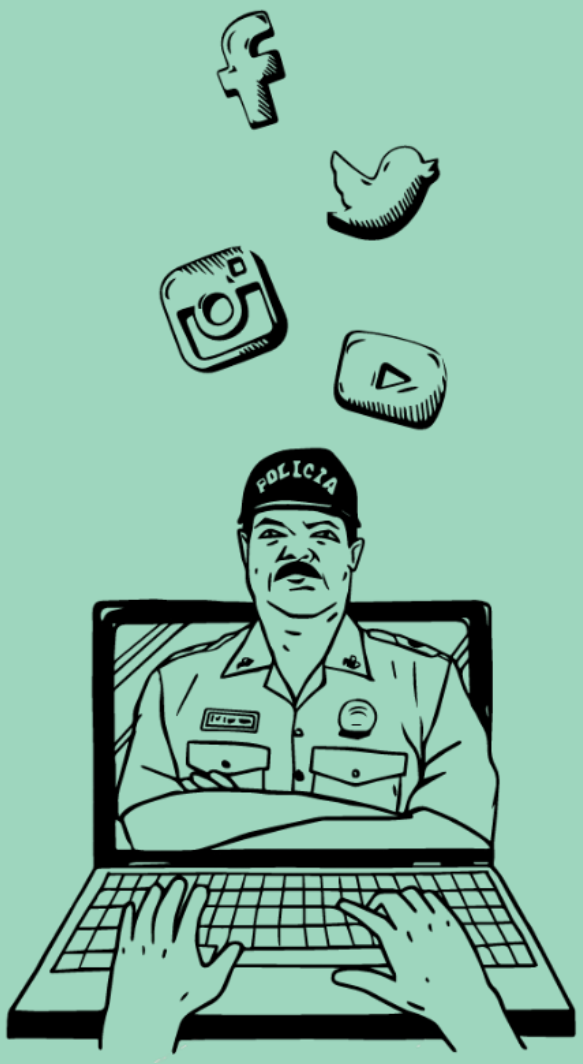
22 Frederick Schauer (1978). Fear, Risk and the First Amendment: Unraveling the "Chilling Effect".

23 Penney, J. W. (2017). Internet surveillance, regulation, and chilling effects online: A comparative case study. Internet Policy Review, 6(2). https://doi.org/10.14763/2017.2.692

24 CIDH, RELE y OACNUDH (2022). "La CIDH, RELE y OACNUDH expresan preocupación ante los hallazgos sobre uso del software Pegasus para espiar a periodistas y organizaciones de la sociedad civil en El Salvador". Disponible en: https://www.oas.org/es/cidh/jsForm/?File=/es/cidh/prensa/comunicados/2022/022.asp

Como se observa, la vigilancia estatal y sus efectos impactan de forma directa sobre el libre intercambio de ideas que una sociedad democrática debe proteger y promover. Este derecho no solo es clave para el ejercicio ciudadano, sino que cuenta con reconocimiento expreso tanto en la normativa nacional como en los estándares internacionales de derechos humanos. En el caso del Perú, está reconocido en el artículo 2.2. de la Constitución, que garantiza "las libertades de información, opinión, expresión y difusión del pensamiento mediante la palabra oral o escrita o la imagen, por cualquier medio de comunicación social, sin previa autorización ni censura ni impedimento algunos". A nivel internacional, tanto la Convención Americana como el Pacto de Derechos Civiles y Políticos reconocen que este derecho comprende "la libertad de buscar, recibir y difundir informaciones e ideas de toda índole".

CAPÍTULO 2: EL ECOSISTEMA DE LA VIGILANCIA ESTATAL



En el Perú, hay diversos escenarios, contextos y situaciones en las que las entidades públicas, cada una desde su rol, pueden desplegar acciones de vigilancia. En este apartado se hará una revisión de cada una de ellas, agrupada según el sector en el que operan.

1. VIGILANCIA EN EL SISTEMA PENAL

En el ámbito penal, se despliegan acciones de vigilancia con fines de investigación y prevención del delito, ya sea para identificar a uno o más individuos responsables de la comisión de un ilícito penal, o para identificar potenciales escenarios de acción delictiva. Para ello, intervienen principalmente cuatro actores:

- **Ministerio Público**: Es el titular de la acción penal pública, que ejerce de oficio, a solicitud de la parte agraviada o por acción popular[1]. En consecuencia, representa a la sociedad en el juicio penal. Además, conforme al artículo 250.5 de la Constitución, vigila e interviene en la investigación del delito desde la etapa policial, orien-

[1] Artículo 11 de la Ley Orgánica del Ministerio Público.

tándola en cuanto a las pruebas y al cumplimiento del marco legal. De manera análoga, cumple funciones en las acciones policiales preventivas del delito[2].

- **Policía Nacional del Perú:** Es la institución encargada de ejercer la función policial en todo el territorio nacional, con competencia administrativa y autonomía operativa. Su función general es garantizar, mantener y restablecer el orden interno y el orden público. Para efectos de este informe, resulta especialmente relevante su rol en la prevención, investigación y denuncia de delitos, así como en la obtención y custodia de evidencias. Aunque actúa como órgano ejecutor en materia de orden interno y público, muchas de sus acciones se rigen por protocolos y directivas elaboradas y aprobadas por el Ministerio del Interior, entidad de la que depende orgánicamente por estar adscrita a ella.
- **Juez de Investigación Preparatoria**: Durante la etapa de investigación, este juez actúa como juez de garantías. No se trata del mismo juez que decide en juicio oral sobre la responsabilidad penal del acusado. Su tarea es autorizar, supervisar y controlar los actos de investigación dirigidos por el Ministerio Público cuando estos puedan limitar o afectar derechos fundamentales. Dado que esta etapa está orientada a reunir los elementos de convicción que permitan acusar (o no) al imputado, la participación del juez resulta esencial para equilibrar la investigación con la protección de derechos.
- **Juez Penal:** Es el encargado de dirigir el juicio oral y decidir si el acusado es culpable o inocente. Sin embargo, también puede intervenir en la etapa de investigación. En situaciones de emergencia que amenacen la vida, integridad o libertad personal de una víctima, el Fiscal puede solicitar directamente al Juez Penal el levantamiento del secreto de las comunicaciones, como se explicará en la siguiente sección.

Estos actores tienen diversas habilitaciones legales y competencias para ordenar, ejecutar o controlar medidas orientadas a la ob-

[2] Artículo 9 de la Ley Orgánica del Ministerio Público.

tención de información privada, las cuales permiten acceder a la ubicación en tiempo real de una persona o interceptar sus llamadas telefónicas, por ejemplo. A continuación, se ofrece un resumen de cada una de ellas.

1.1. Intervención y control de las comunicaciones

El procedimiento aplicable a cualquier forma de intervención de las comunicaciones está normado en la Ley 27697, "Ley que otorga facultad al Fiscal para la intervención y control de comunicaciones y documentos privados en Caso Excepcional", así como el Código Penal y el Código Procesal Penal.

Ley 27697 (2002)

Esta normativa desarrolla legislativamente la facultad constitucional otorgada a los jueces para conocer y controlar las comunicaciones de las personas que son materia de investigación preliminar o jurisdiccional[3]. Según el artículo 1 de la referida norma, esta facultad solo puede ejercerse respecto de los siguientes delitos:

- Secuestro
- Trata de personas
- Pornografía infantil
- Robo agravado
- Extorsión
- Tráfico ilícito de drogas
- Tráfico ilícito de migrantes
- Delitos contra la humanidad (que incluyen el genocidio, la desaparición forzada, la tortura, la discriminación y la manipulación genética)
- Atentados contra la seguridad nacional y traición a la patria
- Peculado

[3] Artículo 1 de la Ley 27697. Disponible en: https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H824116

- Corrupción de funcionarios
- Terrorismo
- Delitos tributarios y aduaneros
- Lavado de activos
- Delitos informáticos (tipificados en la Ley 30096, que incluye, entre otros, el acceso ilícito, la interceptación de datos informáticos, las proposiciones sexuales a NNA por medios tecnológicos, el fraude informático, etc.).
- Delitos relacionados con la explotación sexual y el proxenetismo.

Para este procedimiento, el Fiscal de la Nación, Fiscal Penal o Procurador Público, cuando corresponda, está a cargo de presentar la solicitud de intervención de las comunicaciones al juez en los casos materia de su investigación. Esta solicitud debe estar debidamente sustentada y contener datos completos, anexando, además, los elementos indiciarios que le permitan al juez autorizar (o no) la medida requerida. Para ello, es importante que se precise si la comunicación (i) es determinada o no; (ii) si se tiene certeza que sucederá dentro de ciertas circunstancias; (iii) si es pasada o futura; (iv) si es accesible a cualquier persona que la perciba, o si, al contrario, está encriptada o cerrada; (v) si ha sido objeto de medios destinados a encubrir la identidad del emisor o receptor; entre otros.

Estos factores también deben estar especificados en la resolución de autorización que realice el juez, a fin de que sea posible distinguir las distintas clases de recolección y de control que se realizarán. Además, la autorización del Juez debe incluir un plazo —que no puede superar los 60 días en el caso de la intervención de las comunicaciones—, el cual es excepcionalmente prorrogable por plazos sucesivos cuando el Fiscal lo solicite.

La ejecución de la intervención y control de las comunicaciones está a cargo del personal autorizado del Ministerio Público y/o la Policía Nacional del Perú, bajo supervisión del Fiscal. Todos estos actores, incluyendo también al personal auxiliar, los Procuradores Públicos, el Juez, y demás personas autorizadas en el proceso de investigación deben guardar reserva sobre toda la información que obtengan.

En adición, otro actor relevante para que se pueda realizar este procedimiento son las empresas de comunicaciones: sobre ellas recae la obligación de facilitar en tiempo real el control o recolección de las comunicaciones inmediatamente después de recepcionada la resolución judicial de autorización.

Código Procesal Penal (2004)

El Título III del Código Procesal Penal (CPP) regula la búsqueda de pruebas y la restricción de derechos, estableciendo los límites y condiciones bajo los cuales puede afectarse la privacidad de las personas durante una investigación penal. En este marco, el Capítulo VII está dedicado al control de las comunicaciones y documentos privados, y su Subcapítulo II aborda específicamente la intervención de comunicaciones y telecomunicaciones como técnica especial de investigación.

Dentro de esta regulación, el artículo 230 del CPP norma la intervención, grabación o registro de comunicaciones telefónicas o de otras formas de comunicación y geolocalización de teléfonos móviles. A diferencia de la Ley 27697, este dispositivo legal establece que el Fiscal puede solicitar la medida cuando existan motivos para considerar la comisión de un delito *sancionado con pena superior a los cuatro años de privación de libertad*. Además del estándar probatorio mínimo, la norma exige que la intervención sea absolutamente necesaria para el avance de la investigación, lo cual introduce un requisito de proporcionalidad.

El Juez de la Investigación Preparatoria es el encargado de autorizar la medida mediante una resolución motivada. Esta puede dirigirse directamente contra el investigado o contra terceras personas que, según información objetiva, transmitan o reciban comunicaciones por cuenta de él, o que usen medios que se presume están siendo utilizados por el investigado. En este sentido, la norma contempla expresamente una amplitud tecnológica, abarcando cualquier sistema o plataforma de comunicación: radial, telefónica, satelital, digital, por internet, entre otros soportes que entren en la categoría de tecnologías de la información y las comunicaciones (TIC).

El requerimiento fiscal, así como la resolución judicial que lo auto-

rice, debe contener información detallada sobre el sujeto afectado por la medida (en caso de conocerse), la identificación del medio o dispositivo que será intervenido, el alcance y la duración de la interceptación, y los datos del personal encargado de ejecutar la diligencia.

El artículo también prevé un procedimiento excepcional para situaciones de emergencia que impliquen una amenaza inminente contra la vida, la integridad o la libertad personal de la víctima. En estos casos, el Fiscal podrá solicitar la medida directamente al Juez Penal dentro de las 24 horas desde la recepción del informe policial. El Juez, a su vez, deberá resolver también en un plazo máximo de 24 horas, y en caso de proceder, requerirá directamente la información a las operadoras, quienes deben entregarla en ese mismo periodo tanto al Ministerio Público como a la unidad policial responsable.

Las empresas de telecomunicaciones tienen obligaciones específicas dentro de este marco: deben brindar asistencia inmediata para la ejecución de la medida, incluyendo la geolocalización en tiempo real, las 24 horas del día, todos los días del año. Asimismo, están obligadas a garantizar la compatibilidad tecnológica con el Sistema de Intervención y Control de las Comunicaciones de la Policía Nacional del Perú. Esta compatibilidad debe mantenerse incluso cuando actualicen o renueven sus equipos y software.

La intervención tiene un plazo máximo de 60 días, prorrogable por única vez y por el mismo periodo, siempre que el Fiscal lo sustente con nuevos elementos probatorios y el Juez lo apruebe mediante resolución motivada. La medida también puede cesar antes si pierde relevancia para la investigación o si los elementos de convicción que la justificaban desaparecen. En todos los casos, la decisión de interrumpir la intervención recae en el Fiscal, quien asume responsabilidad funcional por esta determinación.

El artículo 231 añade que el Fiscal tiene la potestad de conservar las grabaciones hasta que culmine el proceso penal —o al finalizar la investigación si esta no se judicializa—, previa autorización del juez. Además, este artículo también establece la obligación de notificar a el o los investigados sobre todo lo actuado (grabaciones, geolocalización, etc.), solo si el objeto de la investigación lo

permite y en tanto esto no ponga en peligro la vida o la integridad corporal de terceros. En sentido contrario, para que la intervención se mantenga en secreto es necesaria una resolución judicial motivada y con plazo determinado.

Protocolo de Actuación Conjunta (2014)

En 2014, el Consejo Ejecutivo del Poder Judicial (Resolución Administrativa N° 134-2014-CE-PJ) y el Ministerio Público (Resolución de la Fiscalía de la Nación N° 1502-2014-MP-FN) aprobaron documentos de gestión con la finalidad de facilitar la labor de dichas instituciones en la investigación y persecución del delito. A fin de articularlos de mejor manera y facilitar su aplicación práctica, el Ministerio de Justicia aprobó los Protocolos de Actuación Conjunta (Resolución Ministerial 243-2014-JUS), entre los que se encuentra el Protocolo para la Intervención o Grabación de Registro de Comunicaciones Telefónicas o de otras formas de Comunicación[4]. Dicho Protocolo detalla de manera más específica cada uno de los pasos del procedimiento y las tareas que realiza cada una de las entidades involucradas.

Así, por ejemplo, el procedimiento inicia con la obtención, por parte de la PNP (en específico, del policía a cargo de la investigación criminal), de datos tales como números telefónicos, SIM, IMSI, IMEI, dirección IP, correos electrónicos y otros datos de las personas involucradas. Esta información podrá ser obtenida mediante acciones de inteligencia y otras "fuentes legítimas".

Luego de verificar estos datos, el policía a cargo puede remitir un Informe al Fiscal, a través del cual solicita la obtención del mandato de intervención. Este informe debe contener el hecho investigado, los indicios, las razones de la necesidad de la intervención, la forma de interceptación pertinente y la dependencia policial que estaría encargada de ejecutar la diligencia. Aquí se especifica que cuando se requieran intervenciones en tiempo real, monitoreo remoto y geolocalización, se designará a la Oficina de Apoyo Técnico Judicial de la PNP, la cual "tiene a cargo el componente de Gestión

[4] Disponible en https://spij.minjus.gob.pe/Graficos/Peru/2014/Noviembre/13/RM-243-2014-JUS.pdf, p. 8ss.

de Datos y Contenido de las Comunicaciones en los Sistemas de Intervención de Comunicaciones"[5].

En el plazo de 24 horas, el Fiscal evalúa el Informe y decide si formalizará el requerimiento ante el Juez competente. Los datos del Informe policial son clave para construir la solicitud, la cual tiene prácticamente el mismo contenido.

En respuesta, el Juez examina la solicitud y emite una resolución mediante un trámite reservado. De hecho, las empresas de telecomunicaciones únicamente reciben la transcripción de la parte resolutiva y el número telefónico o dato intervenido. En adelante, el Protocolo detalla las acciones de ejecución (conservación y registro de datos, coordinación entre Fiscalía y PNP, transcripción de grabaciones, etc.) y de control posteriores.

Es importante resaltar que este Protocolo distingue entre la intervención de comunicaciones regulada por la Ley N.º 27697 y la prevista en el Código Procesal Penal (ambas abordadas previamente). Aunque son procedimientos muy similares, son de aplicación en diferentes contextos. En el primer caso, se aplica cuando la investigación sigue el Código de Procedimientos Penales de 1940 o la Ley Contra el Crimen Organizado (Ley N.º 30077), y está referida a los delitos enumerados en el artículo 1 de la Ley 27697 —los cuales pueden consultarse en esta sección—. En cambio, el artículo 230 corresponde al marco del "Nuevo" Código Procesal Penal (2004), y es aplicable cuando el delito imputado tiene una pena superior a cuatro años de privación de libertad. En este segundo supuesto, el criterio es temporal y cuantitativo (la pena), no una lista cerrada de delitos.

1.2. Geolocalización

Aunque el acceso a la geolocalización puede darse en el marco de la intervención de comunicaciones, como se vio en la sección anterior, en este apartado se analiza un supuesto particular: la geolocalización habilitada mediante el Decreto Legislativo (DL) 1182, también conocido como Ley Stalker, y su modificación posterior a

[5] Protocolo de Actuación Conjunta, p. 13.

través de la Ley 31284[6]. Se trata de un mecanismo independiente del régimen anterior porque no requiere orden judicial previa, sino que lo ejecuta directamente la Policía Nacional del Perú (PNP).

En un primer momento, esta norma se presentó como una respuesta a la crisis de criminalidad en el país. Bajo el discurso de la necesidad de actuar de manera ágil frente a delitos en flagrancia, se creó un régimen paralelo al previsto en el Código Procesal Penal, que prescinde de la autorización judicial previa bajo el argumento de su carácter excepcional.

Sin embargo, en 2021 se ampliaron sus alcances de manera significativa[7]. Mientras que antes solo podía aplicarse para delitos en flagrancia sancionados con una pena mayor a cuatro años de prisión, tras su modificación se eliminó el requisito de flagrancia. Actualmente, el acceso a la geolocalización sin orden judicial es procedente en investigaciones preliminares vinculadas a delitos contra la vida, el cuerpo y la salud; delitos contra la libertad; delitos contra el patrimonio; delitos contra la administración pública; lavado de activos; trata de personas; tráfico ilícito de drogas; minería ilegal; y los delitos comprendidos en la Ley 30077, Ley contra el Crimen Organizado.

A diferencia del procedimiento ordinario revisado previamente —que también puede aplicarse para estos delitos—, el DL 1182 establece que tanto el fiscal como el juez toman conocimiento de la medida después de su ejecución. En la práctica, la PNP solicita directamente a las empresas de telecomunicaciones el acceso a los datos de ubicación, y posteriormente requiere al Ministerio Público que solicite la convalidación judicial. Esta debe resolverse mediante trámite reservado y de forma inmediata, en un plazo máximo de 24 horas. La duración de la medida puede ser de hasta 60 días, prorrogables.

En adición, la norma impone a las empresas de telecomunicaciones

---

6 Disponible en: https://leyes.congreso.gob.pe/Documentos/2016_2021/ADLP/Normas_Legales/31284-LEY.pdf

7 León, Lucía (2021). "Congreso amplía los alcances de la problemática Ley Stalker o Ley de Geolocalización". Disponible en: https://hiperderecho.org/2021/07/congreso-amplia-los-alcances-de-la-problematica-ley-stalker-o-ley-de-geolocalizacion/

la obligación de conservar los datos derivados de las comunicaciones. Estos deben almacenarse durante un año en sistemas informáticos que permitan su consulta y entrega en línea y en tiempo real. Luego, las empresas deben conservar dicha información por dos años más en un sistema de archivo electrónico, a disposición de las autoridades competentes.

1.3. Agentes encubiertos en entornos digitales

Código Procesal Penal

El Código Procesal Penal prevé la existencia de técnicas especiales de investigación, reguladas, principalmente, en el artículo 341. Inicialmente, cuando se promulgó esta norma (aprobada por DL 957[8]), el art. 341 trataba únicamente sobre agentes encubiertos. Luego se amplió su alcance y se creó la figura del agente especial. En la actualidad, con una modificación realizada en diciembre de 2023 (DL 1611[9]), son 4 las figuras reguladas de técnicas especiales de investigación, las cuales deben cumplir con los requisitos de idoneidad y necesidad, además de ser indispensables para el esclarecimiento de los hechos investigados (i) perpetrados por banda u organización criminal, en el marco de lo que indica la Ley 30077; (ii) por delitos de trata de personas; o (iii) por delitos contra la administración pública, según se prevee en los artículos 382-401 del Código Penal. Estas 4 figuras son las siguientes:

- "**Agente encubierto**: Ejecutado por miembro de la Policía Nacional del Perú en situación de actividad perteneciente a la unidad especializada competente, que reúna las condiciones necesarias para establecer contacto o infiltrarse en una banda u organización criminal.
- **Agente Especial**: Realizado por elemento captado debido al rol, conocimiento o vinculación con actividades ilícitas, a fin de establecer contacto o insertarse en la actividad de banda u organización criminal, proporcionando información o las

[8] Disponible en: https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H682695
[9] Disponible en: https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H1365316

evidencias incriminatorias de aquellas; bajo el monitoreo directo de la autoridad policial.

- **Agente Revelador**: Realizado por cualquier ciudadano, o por servidor o funcionario público, que, como integrante o miembro de una banda u organización criminal, actúe proporcionando información o las evidencias incriminatorias de aquellas; bajo el monitoreo directo de la autoridad policial.
- **Agente virtual**: Realizado por personas debidamente entrenadas en materias de tecnología de la información y las comunicaciones, así como, los conocimientos y habilidades correspondientes con la finalidad de asumir un rol o condición a efecto del esclarecimiento de delitos en el ámbito virtual; bajo el monitoreo directo de la autoridad policial".

Cualquiera de estos agentes está exento de responsabilidad penal por las actuaciones necesarias para el desarrollo de la investigación, siempre que sean proporcionales a la finalidad de la misma y no constituyan una provocación manifiesta al delito.

El procedimiento para registrar, elegir y administrar de manera reservada los agentes, incluyendo los requisitos y cualidades que deben cumplir, las actividades, el tráfico jurídico o social en el que se desenvuelven, así como otras previsiones técnicas y jurídicas, se regula mediante Decreto Supremo, según dispone el Código Penal. No obstante, a la fecha no existe una norma como tal aprobada.

Estas técnicas especiales de investigación concuerdan con lo dispuesto en el artículo 10 del DL 1611, según el cual la PNP, para la investigación del delito de extorsión y delitos conexos, recomienda la estrategia de investigación al Fiscal. En el marco de ello, la PNP puede ejecutar

> "acciones de observación, *vigilancia* y *seguimiento físico o remoto*, respecto a personas o en torno a objetos o inmuebles, tendentes a la identificación o individualización de sujetos, localización de implicados en el ilícito penal o víctimas del delito, descubrimiento de centro de operaciones ilícitas, modus operandi, vínculos, estructuras criminales y otras razones relacionadas con el recaudo de los elementos materiales de convicción debidamente registradas y acreditadas en acta".

Además, la PNP debe sustentar los informes de requerimiento al Fiscal para la ejecución de estas técnicas especiales de investiga-

ción (así como otras, tales como el levantamiento judicial del secreto de las comunicaciones desarrollado previamente).

Legislación especial

Además del Código Procesal Penal, existen dos leyes especiales que prevén la ejecución de este tipo de técnicas especiales de investigación. Al ser previas a la modificación del 2023, se enfocan únicamente en la figura de "Agente encubierto", aunque con ciertos matices particulares:

- **Ley contra el Crimen Organizado**[10] (2013, modificada en 2023): En su artículo 13, la norma señala que los agentes encubiertos están facultados para participar en el tráfico jurídico y social, adquirir, poseer o transportar bienes de carácter delictivo, permitir su incautación e intervenir en toda actividad útil y necesaria para la investigación del delito que motivó la diligencia, luego de emitida la disposición fiscal que autoriza su participación. Además, la ley remite al Código Procesal Penal, al referirse a lo dispuesto en el artículo 341 previamente analizado.
- **Ley de Delitos Informáticos**[11] (2013, modificada en 2023): Esta norma, en su segunda disposición complementaria final, crea por primera vez la figura de "agente encubierto en entornos digitales". Así, reitera la facultad del fiscal para autorizar la actuación de agentes encubiertos a efectos de realizar las investigaciones de los delitos que se cometan mediante tecnologías de la información y las comunicaciones, incluso si estas acciones encubiertas deben realizarse en entornos digitales. En ese sentido, se amplían los alcances del Código Procesal Penal, que reservaba esta técnica especial de investigación a ciertos delitos (cometidos por banda organizada, trata de personas o delitos contra la administración pública).

  Con la modificación de 2023, la norma también establece

[10] Ley 30077. Disponible en: https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H1084545

[11] Ley 30096. Disponible en: https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H1088463

> que los protocolos para la actuación del agente encubierto en entornos digitales son coordinados, en cuanto corresponda, con la Secretaría de Gobierno y Transformación Digital.

Una de las cuestiones que llama la atención es que en 2023 se realizaron diversas modificaciones a este marco legal: por un lado, se crea la figura de "agente encubierto en entornos digitales", además de la disposición de coordinación de sus protocolos con el ente rector en transformación digital del país (la SGTD); por otro lado, se crea la figura de agente virtual en el Código Procesal Penal. Lamentablemente, no queda claro si se trata de la misma figura (por la similitud nominal), lo cual sería importante pues el agente virtual del CPP no es necesariamente un agente PNP, aunque sí debe contar con supervisión policial.

El artículo 43 de la Ley de la Policía Nacional del Perú (Decreto Legislativo 1267), referido al empleo de sistemas tecnológicos y registros con fines policiales, habilita su uso para "sistemas de patrullaje virtual". Sin embargo, la norma no precisa los alcances de esta facultad ni existe un protocolo público que permita evaluar si se cumplen estándares en materia de derechos humanos. En la práctica, algunas providencias muestran que el procedimiento habitual consiste en designar agentes para realizar patrullaje en redes sociales —como Facebook, YouTube o mediante búsquedas en Google— con el fin de extraer información, audios, videos y otros datos relevantes para la investigación de delitos[12]. La labor del Departamento de Patrullaje Virtual, no obstante, se extiende más allá de las redes sociales, incluyendo la revisión de sistemas internos de la PNP, como el Sistema Nacional de Registro de Denuncias de Investigación Criminal (SIRDIC)[13].

---

[12] Ver, por ejemplo, la providencia publicada en https://lpderecho.pe/en-que-consiste-el-patrullaje-virtual-policia-nacional-del-p

[13] Ver, por ejemplo, este informe: https://cdn.www.gob.pe/uploads/document/file/7910441/6659489-informe-denuncias-falsas-en-sirdic-2.pdf?v=1744340170

2. VIGILANCIA EN EL ÁMBITO DE INTELIGENCIA

El Sistema Nacional de Inteligencia (SINA) es el conjunto de entidades, normas, procedimientos y recursos del Estado peruano dedicados a la producción de inteligencia estratégica, militar y policial[14], así como a actividades de contrainteligencia. Su función principal es generar conocimiento útil para la toma de decisiones en materia de seguridad nacional[15]. A nivel funcional, el SINA está bajo la dirección de la Dirección Nacional de Inteligencia (DINI), una entidad adscrita directamente a la Presidencia del Consejo de Ministros, lo que refuerza su carácter central y político, al margen de la estructura de cualquier ministerio específico.

El marco legal principal del sistema es el Decreto Legislativo 1141, promulgado en 2012. Esta norma define la inteligencia como una "actividad que comprende un proceso sistemático de búsqueda, evaluación y análisis de información, cuya finalidad es producir conocimiento útil para la toma de decisiones"[16]. Se trata de una definición amplia e imprecisa, que no establece límites claros respecto al tipo de información que puede recolectarse ni sobre los métodos empleados para hacerlo. Sin embargo, por el contexto de su aplicación —el ámbito gubernamental y de seguridad—, queda claro que se refiere a actividades de alto nivel de secretismo, centradas en identificar o monitorear amenazas reales o potenciales a los intereses estratégicos del Estado[17].

Una de las características más llamativas del SINA es precisamente el elemento de opacidad, que no sólo es tolerado por el marco legal, sino que está formalmente instituido como uno de sus principios rectores. La norma establece el principio de *circulación restringida*, según el cual toda información vinculada a la actividad de

---

14 Artículo 7.1. del DL 1141, Decreto Legislativo de Fortalecimiento y Modernización del Sistema de Inteligencia Nacional - SINA y de la Dirección Nacional de Inteligencia - DINI.

15 Artículo 8.1. del DL 1141.

16 Artículo 2.1. del DL 1141.

17 Shulky, Abraham N., y Schmitt, Gary J., Silent Warfare (2002). Understanding the world of intelligence, 3a ed., Brassey's Inc., Washington D.C., p. 1

inteligencia tiene un acceso limitado únicamente a entidades públicas expresamente autorizadas. Este blindaje legal convierte a la inteligencia en uno de los espacios menos transparentes del aparato estatal, incluso frente a otros órganos de control y rendición de cuentas. Es razonable que por motivos de seguridad interna y externa, el sector inteligencia cuente con mayores filtros para acceder a su información. No obstante, debemos preguntarnos cuál es el límite de esta excepción al principio de transparencia que rige el aparato estatal.

En específico, los componentes del SINA (Dirección Nacional de Inteligencia - DINI como ente rector, junto con las Direcciones de Inteligencia respectivas de sectores como Relaciones Exteriores, Defensa e Interior) ejecutan *procedimientos especiales de obtención de información* para obtener información "estrictamente indispensable para el cumplimiento de los objetivos de la actividad de inteligencia"[18].

La DINI tiene entre sus funciones, precisamente, establecer los procedimientos especiales para la obtención de información en entornos digitales y para peritajes informáticos. Para su diseño, puede suscribir convenios interinstitucionales con el Poder Judicial, a fin de recibir asesoría técnica.

La ejecución de un procedimiento especial requiere, como regla general, autorización judicial previa. Esta es otorgada por uno de los dos jueces superiores *ad hoc* designados por la Corte Suprema, en un plazo máximo de 24 horas desde la recepción de la solicitud. Todo el proceso tiene carácter de información clasificada como "secreta" —aspecto que se desarrollará en el capítulo 3—, y la autorización es vinculante para cualquier entidad pública que deba colaborar, bajo las disposiciones sobre manejo de información clasificada.

La solicitud, presentada por el Director de la DINI, debe identificar a la persona o personas afectadas, detallar las medidas solicitadas y precisar su motivación y duración. No obstante, hay un caso excepcional en el que no se requiere autorización judicial previa: cuando exista un peligro contra la seguridad nacional y la urgencia

[18] Artículo 33 del DL 1141.

lo justifique, el Director de la DINI puede ordenar la ejecución inmediata del procedimiento, con cargo a formalizar la solicitud ante el juez competente de forma inmediata. Este deberá convalidar o suspender la medida en un plazo máximo de 24 horas[19].

Aunque la norma no precisa en qué consisten ni ofrece ejeplos de los *procedimientos especiales de obtención de información*, es evidente que su aplicación implica una injerencia en el derecho a la privacidad. El hecho de que las solicitudes de autorización deban identificar expresamente a la persona *afectada* confirma que estas medidas conllevan, de forma inevitable, una vulneración de dicho derecho.

Es importante precisar, además, que los informes de inteligencia pretenden ser empleados en este contexto. En ese sentido, la norma señala que en ningún caso los informes de inteligencia tendrán valor probatorio dentro de procesos judiciales, administrativos y/o disciplinarios —aunque sí podrían servir para orientar la investigación—.

Por otra parte, la norma prevé que toda información obtenida para la producción de inteligencia por el SINA, que sea innecesaria para el objetivo del sistema por corresponder a los derechos fundamentales y a la esfera de la vida privada, debe ser destruida por los funcionarios responsables de los componentes del sistema que la detenten, bajo responsabilidad[20]. No obstante, no se establece ninguna acción de supervisión o control para verificar la eliminación de esta información.

La norma sí establece ciertos espacios de control generales —es decir, no para cuestiones específicas como la anteriormente mencionada—. Por un lado, la Comisión de Inteligencia del Congreso (art. 36) puede requerir información clasificada y no clasificada directamente a todos los componentes del SINA, así como iniciar o disponer investigaciones de oficio y solicitar información clasificada a los jueces superiores *ad hoc*. La Contraloría General de la República, por su parte, realiza el control gubernamental de la gestión administrativa, económica y financiera de los recursos y

[19] Artículo 33.5 del DL 1141.

[20] Art. 35 del DL 1141.

bienes de los componentes del SINA, incluso cuando se trate de recursos especiales. Además, la Contraloría realiza un informe anual sobre estas acciones de control, el cual debe presentar ante la referida Comisión de Inteligencia del Congreso.

3. MONITOREO EN EL SECTOR DE TELECOMUNICACIONES

A diferencia de las facultades de vigilancia directa y de interceptación legalmente habilitadas para entidades como la Policía Nacional del Perú (PNP) y el Ministerio Público en el ámbito penal y de inteligencia, el Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL) opera en un rol regulatorio distinto. Sin embargo, su capacidad para acceder a datos georreferenciados y personales de los usuarios de los servicios de telecomunicaciones sitúa a la entidad en una posición que plantea serias dudas en materia de privacidad y transparencia. Si bien OSIPTEL no realiza actividades de vigilancia *per se*, su acceso a información sensible de los ciudadanos puede ser objeto de escrutinio, especialmente en un contexto donde el ecosistema de vigilancia en el Perú evoluciona constantemente.

Las facultades de OSIPTEL para obtener datos de los usuarios se derivan, entre otras, de su labor de fiscalización de la calidad del servicio de los operadores móviles. Para este fin, la entidad ha diseñado una serie de herramientas de medición que recopilan una gran cantidad de datos, incluyendo la ubicación geográfica precisa de los dispositivos. Según la Norma Técnica relativa a la implementación del sistema de medición automatizado para la verificación del servicio de acceso a internet por parte del OSIPTEL[21], los operadores están obligados a proporcionar a OSIPTEL acceso a esta información.

La recopilación de datos se lleva a cabo a través de dos mecanismos principales:

[21] Aprobada por Resolución de Consejo Directivo 137-2021-CD/OSIPTEL y modificada por Resolución de Consejo Directivo N.º 178-2023-CD/OSIPTEL.

- **API en routers:** OSIPTEL ha establecido que las empresas de telecomunicaciones utilicen un API (interfaz de programación) instalado en los routers para recolectar información sobre el rendimiento del internet fijo en los hogares. Aunque su objetivo es medir la calidad del servicio, este software también podría acceder a otros datos relacionados con la red.
- **Aplicaciones móviles:** En el caso del internet móvil, se dispuso que las operadoras incluyan un SDK (módulo de software) dentro de sus aplicaciones oficiales. Este componente permite monitorear la calidad del servicio mientras las personas usan la app para revisar su plan, pagar recibos u otras gestiones, lo que amplía la capacidad de las empresas para recopilar datos del usuario.

Mediante estos mecanismos, los operadores deben recoger y procesar diversos parámetros de información, los cuales entrega a OSIPTEL en una base de datos denominada "Registro de Abonados". Este registro incluye datos como el número de teléfono, IMEI del equipo, IMSI del chip, , ubicación georeferenciada (latitud y longitud), y más datos asociados al nombre completo de la persona, el cual es un dato obligatorio que no puede ser dejado en blanco.

Según la norma técnica, OSIPTEL recibe una actualización semanal de este Registro, el cual debe ser cargado en el Sistema de Medición. Esto genera una serie de preocupaciones fundamentales sobre la privacidad y la protección de datos, ya que la información recolectada no se limita a métricas técnicas de calidad del servicio: incluye una actualización semanal de la geolocalización de todas las personas con líneas activas, con 5 decimales de exactitud, lo cual permitiría hacer un mapa de movimientos a gran escala.

Aunque se especifica que esta transferencia de datos sería anónima, de acuerdo al procedimiento que se utilice, los datos anonimizados pueden ser fácilmente reidentificados, peor aún si consideramos que en el Perú las líneas telefónicas solo se pueden obtener mediante autenticación por huella dactilar, lo que hace plenamente identificable un número de teléfono con una persona específica.

En este sentido, el caso de OSIPTEL ilustra una zona gris dentro del ecosistema de vigilancia en el Perú. Si bien la justificación de la recopilación de datos es la supervisión técnica, la magnitud de la información personal y georreferenciada a la que tiene acceso la pone en una situación de potencial riesgo. El marco legal que le da estas facultades no logra establecer garantías suficientes que aseguren que los datos no puedan ser mal utilizados, accidentalmente expuestos o solicitados por otras entidades estatales con fines de vigilancia, sin los controles estrictos que rigen el ámbito penal o de inteligencia. Por ello, la posición de OSIPTEL merece una atención especial en un análisis integral de la vigilancia en el país.

CAPÍTULO 3: TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA

La transparencia es un componente esencial para garantizar el control democrático de las instituciones y el respeto de los derechos fundamentales. En el ámbito de la vigilancia estatal y la obtención de información, su importancia se multiplica: sin mecanismos que permitan conocer el alcance, la legalidad y los resultados de estas prácticas, se corre el riesgo de que se desarrollen en la opacidad y sin rendición de cuentas.

En este capítulo se analizará cómo el marco legal peruano regula el acceso a la información pública, cuáles son los límites y excepciones a este derecho y cómo estas barreras se relacionan con la afectación a derechos como la privacidad y la libertad de expresión en contextos de vigilancia.

1. TRANSPARENCIA Y DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA

El *principio de transparencia* es un pilar del sistema democrático mediante el cual toda actuación del Estado debe ser accesible a las personas. Este principio garantiza la posibilidad de control por parte de la ciudadanía sobre las acciones y decisiones que toma

el Estado —a través de los distintos poderes públicos y organismos—. Esto no siempre fue así: se requirió un cambio de paradigma importante para reconocer que el Estado debe cumplir con el deber de transparencia, frente a la cultura del secreto previa imperante en la Administración Pública[1].

En la actualidad, es indiscutible que la transparencia constituye un valor fundamental del Estado democrático de Derecho, el cual tiene efectos positivos importantes en la sociedad. En primer lugar, tiene un rol crucial en la lucha contra la corrupción: a mayor disponibilidad de información y mayores estándares de publicidad, es más sencillo detectar malas prácticas. De ahí, por ejemplo, que el componente de "transparencia, datos abiertos y rendición de cuentas" sea uno de los más importantes del Modelo de Integridad y Lucha contra la Corrupción vigente[2].

En segundo lugar, la transparencia favorece un mayor involucramiento de la ciudadanía en los asuntos públicos. Al contar con información suficiente y oportuna, las personas pueden ejercer un escrutinio más informado, participar en la toma de decisiones y exigir rendición de cuentas a las autoridades. Este círculo virtuoso fortalece la legitimidad institucional y contribuye a una democracia más participativa.

Finalmente, la transparencia tiene un valor importante para la construcción de un Estado más eficiente. Una cultura de datos abiertos y accesibles permite disponer de información de calidad que, si además es interoperable, mejora la capacidad de respuesta frente a problemas públicos. Esto no solo facilita la identificación de dónde se concentran los desafíos más urgentes, sino que también habilita soluciones basadas en evidencia, optimizando el uso de recursos públicos y evitando duplicidades o ineficiencias.

En virtud de esto, el propio Tribunal Constitucional ha reconocido que se trata de un principio de relevancia constitucional *implícito* en el modelo de Estado democrático y social de Derecho y de la

---

1 Cairampoma Huillca (2025). "Desafíos en la Promoción y Fortalecimiento de la Transparencia: Un Análisis del Rol de los Órganos Garantes de la Transparencia y el Derecho de Acceso a la Información Pública en el Perú, 2018-2024".

2 Disponible en: https://www.gob.pe/31727-presidencia-del-consejo-de-ministros-modelo-de-integridad-publica

fórmula republicana de gobierno[3]. Aunque no exista un precepto constitucional que lo mencione expresamente, este principio se encuentra en la base de la legitimidad del ejercicio del poder público y ha recibido un desarrollo legal importante. Precisamente, es este principio el que da sentido al derecho de acceso a la información pública reconocido en el artículo 2.5 de la Constitución Política del Perú. Dicho artículo establece que toda persona tiene derecho a solicitar —sin necesidad de justificar la causa— la información que requiera y a recibirla de cualquier entidad pública, salvo aquella protegida por la intimidad personal o expresamente excluida por ley por razones de seguridad nacional.

En adición, el propio Tribunal Constitucional del Perú ha precisado que el contenido constitucionalmente protegido de este derecho no se limita al acceso a la información solicitada y a la correlativa obligación de los organismos públicos de entregarla. También exige que la información proporcionada no sea falsa, incompleta, indiciaria o confusa[4], de manera que su entrega cumpla con estándares mínimos de veracidad y calidad.

El desarrollo legislativo de este precepto se encuentra en la Ley 27806, Ley de Transparencia y Acceso a la Información Pública y su Reglamento. Su finalidad, precisamente, es regular el derecho fundamental de acceso a la información pública y promover la transparencia de los actos del Estado. Se trata de la primera norma de alcance general que produjo una regulación aplicable a todas las entidades públicas en materia de acceso a la información.

Esta norma, que data de 2002, establece en su artículo 10 que:

> "Las entidades de la Administración Pública tienen la obligación de proveer la información requerida si se refiere a la contenida en documentos escritos, fotografías, grabaciones, soporte magnético o digital, o en cualquier otro formato, siempre que haya sido creada u obtenida por ella o que se encuentre en su posesión o bajo su control".

En adición, la Ley también considera que cualquier tipo de documentación financiada por el presupuesto público que sirva de base

---

3 STC. Exp. 6070-2009-PHD/TC, fundamento jurídico 5.

4 STC Exp. 1797-2002-HD-/TC, fundamento jurídico 16.

a una decisión de naturaleza administrativa, así como las actas de reuniones oficiales, también constituyen información pública.

Para guiar todo el procedimiento de acceso a la información pública, así como toda actuación o disposición estatal, es imprescindible tener en cuenta el *principio de publicidad*, según el cual:

- Toda información en posesión del Estado se presume pública, salvo las excepciones previstas en la ley.
- El Estado debe adoptar las medidas básicas que garanticen y promuevan la transparencia en la Administración Pública
- El Estado debe entregar la información que requieran las personas en aplicación del principio de publicidad[5].

A nivel transnacional, el Comité Jurídico Interamericano adoptó en 2008 una serie de principios sobre este derecho que también incluyen la presunción de publicidad. A ello se añaden también criterios presentes en nuestra legislación: (i) la extensión de la obligación de entregar la información por parte de todas las entidades públicas en todos los niveles de gobierno; (i) la obligación de implementar reglas justas, claras, no discriminatorias y simples para el manejo de solicitudes de acceso a la información; (iii) el derecho de toda persona de recurrir cualquiera negativa u obstrucción a este derecho; y (iv) la sanción a toda persona que niegue u obstruya su ejercicio violando las reglas que lo garantizan[6].

2. LÍMITES Y EXCEPCIONES

En virtud del principio de publicidad, toda información que posee y/o produce el Estado se presume pública. Naturalmente, como cualquier derecho, el acceso a la información también tiene ciertos límites: no es un derecho absoluto. En ese sentido, una salvedad a la presunción de publicidad es aquellos casos en que se presentan excepciones, las cuales deben estar previstas legalmente.

---

5 Artículo 3 del TUO de la Ley 27806.

6 Disponible en: https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=CJI_9-11

Así lo ha expresado el Tribunal Constitucional, al señalar que, de acuerdo con el principio de máxima divulgación, la publicidad constituye la regla en la actuación de las entidades públicas; y el secreto, cuando cuente con cobertura constitucional, la excepción[7]. Como se observa, este derecho es pasible de restricciones, las cuales se fundamentan en la protección de ciertos bienes o derechos constitucionales[8], que están principalmente regulados en los artículos 15, 16 y 17 de la Ley de Transparencia, los cuales regulan tres tipos de información clasificada: secreta, reservada y confidencial.

Es importante recordar que cualquier restricción de un derecho debe interpretarse restrictivamente. En ese sentido, esta lista de excepciones se trata de una lista taxativa o *numerus clausus*. Además, como señala la Autoridad de Transparencia, en todos los casos, las excepciones deben leerse considerando el daño cierto, real o inminente a los bienes jurídicos que el articulado recoge: es decir, la seguridad nacional, la seguridad de las personas, la integridad territorial y/o la subsistencia del sistema democrático[9].

En suma, deben observarse los siguientes principios al considerar una excepción al acceso a la información pública:

- **Máxima divulgación**: Toda información que posee el Estado se presume pública, salvo las excepciones expresamente previstas. Así, la publicidad constituye la regla y no la excepción.
- **Legalidad de las excepciones:** A las excepciones de los artículos 15, 16 y 17 se pueden sumar otros supuestos de excepción, los cuales deben ser creados por ley aprobada por el Congreso de la República o por Decreto Legislativo (es decir, normas con rango de ley). No se pueden establecer excepciones por normas de menor jerarquía.
- **Taxatividad:** Los supuestos de excepción de la Ley no son ejemplos: son una lista cerrada. Las entidades públicas no pueden aplicar excepciones distintas a las reguladas en la norma.

---

7 STC Exp. N° 2579-2003-HD/TC, fundamento jurídico 5.

8 Opinión Consultiva 02-2020-JUS/DGTAIPD, párrafo 9. Disponible en: https://www.minjus.gob.pe/wp-content/uploads/2020/02/OC-02-1.pdf

9 Opinión Consultiva 25 -2019-JUS/DGTAIPD.

- **Interpretación restrictiva de las excepciones**: En tanto es una limitación a un derecho fundamental, las excepciones se interpretan restrictivamente. No es posible hacer interpretaciones extensivas o por analogía.
- **Proporcionalidad:** Las excepciones deben satisfacer los tres requisitos del test de proporcionalidad, es decir (i) ser idóneas; (ii) ser necesarias; y (iii) ser proporcionales en sentido estricto[10].
- **Temporalidad:** La restricción de acceso a la información opera durante el plazo establecido en la norma o su consiguiente prórroga. No es atemporal.
- **Derechos humanos:** Las entidades no pueden clasificar el acceso a la información relacionada con la violación de derechos humanos en cualquier circunstancia y por cualquier persona (art. 18 de la Ley). Tampoco se considerará de este modo si la misma es utilizada en contra de lo establecido en la Constitución Política[11].

2.1. Información secreta

El artículo 15 de la Ley se refiere a la información secreta, la cual, además, debe estar clasificada como tal en virtud de razones de seguridad nacional (artículo 163 de la Constitución), que además tengan como base fundamental garantizar la seguridad de las personas y cuya revelación originaría riesgo para la integridad territorial y/o subsistencia del sistema democrático, así como respecto a las actividades de inteligencia y contrainteligencia de la DINI.

Esta excepción abarca los siguientes ámbitos:

1. Militar (frente interno y externo): Aquí se incluyen los planes de defensa militar contra posibles agresiones de otros Estados, así como planes logísticos, de reserva y movilización y de operaciones especiales; operaciones y planes de inteligencia y contrainteligencia militar; desarrollos técnicos y/o científicos de defensa militar;

10 STC Exp. 00005-2013-PI/TC, fundamento jurídico 29.

11 Opinión Consultiva 25 -2019-JUS/DGTAIPD.

órdenes de operaciones, logísticas y conexas, relacionadas con planes de defensa militar contra posibles agresiones de otros Estados o de fuerzas irregulares militarizadas internas y/o externas, así como de operaciones en apoyo a la Policía Nacional del Perú, planes de movilización y operaciones especiales relativas a ellas; planes de defensa de bases e instalaciones militares; entre otros.

El límite temporal de esta excepción es de 5 años para la información secreta. Transcurrido ese tiempo, cualquier persona puede solicitar la información. No obstante, si el titular del sector respectivo considera que la divulgación de esta información pone en riesgo "la seguridad de las personas, la integridad territorial y/o subsistencia del sistema democrático", debe sustentarlo expresamente y postergar la clasificación.

2. Inteligencia (frente interno y externo): Se incluyen en este ámbito los planes estratégicos y de inteligencia, así como la información que ponga en riesgo sus fuentes; los informes que, de hacerse públicos, perjudicarían la información de inteligencia; actividades y planes estratégicos de inteligencia y contrainteligencia, de los organismos conformantes del Sistema de Inteligencia Nacional (SINA), así como la información que ponga en riesgo sus fuentes; entre otros.

El DL 1141 de Fortalecimiento y Modernización del Sistema de Inteligencia Nacional - SINA y de la Dirección Nacional de Inteligencia - DINI también contiene disposiciones sobre la clasificación de la información en materia de inteligencia. Así, su artículo 4 señala que es:

> "información clasificada de inteligencia, con el nivel de Secreto, aquella que poseen y/o generan los componentes del Sistema de Inteligencia Nacional - SINA, y que por su naturaleza y contenido constituye una excepción al ejercicio del derecho de acceso a la información pública, en razón de la seguridad nacional, de conformidad con lo establecido en la Ley de Transparencia y Acceso a la Información Pública".

Además, establece 2 supuestos específicos de información clasificada de inteligencia: (i) el detalle de los recursos especiales asignados a los componentes del SINA; y (ii) las resoluciones que autorizan viajes al exterior de personal del SINA.

En el caso de esta información, el DL 1141 señala que su desclasificación, cuando se trate de información relativa a la seguridad nacional, procede a los 20 años. Luego de ello, cualquier persona puede solicitar la información clasificada de inteligencia, la cual podrá ser entregada si el titular del sector o pliego, con opinión favorable del Director de Inteligencia Nacional, considera que su divulgación no constituye riesgo para la seguridad de las personas, integridad territorial y/o subsistencia del sistema democrático; de lo contrario, debe prorrogar la clasificación.

2.2. Información reservada

El artículo 16 también establece como excepción al derecho de acceso a la información pública aquella información clasificada como reservada. Esta excepción comprende los siguientes ámbitos:

1. Orden interno: Información que, por razones de seguridad nacional, originaría un riesgo a la integridad territorial y/o la subsistencia del sistema democrático si se revelara. En consecuencia, se considera reservada la información que tiene por finalidad prevenir y reprimir la criminalidad y cuya revelación podría entorpecer este fin.

Se incluyen en este ámbito los planes de operaciones policiales y de inteligencia, así como aquellos destinados a combatir el terrorismo, tráfico ilícito de drogas y organizaciones criminales; las informaciones que impidan el curso de las investigaciones en su etapa policial dentro de los límites de la ley (como colaboraciones eficaces, sistemas de recompensa y protección de testigos), así como la interceptación de comunicaciones amparadas por la ley; los planes de seguridad y defensa de instalaciones policiales y penitenciarias; el movimiento del personal que pudiera poner en riesgo la vida e integridad de las personas involucradas o afectar la seguridad ciudadana; el armamento y material logístico comprometido en operaciones especiales y planes de seguridad y defensa del orden interno; y la información contenida en Reportes de actividades en relación con sustancias químicas.

2. Relaciones externas del Estado: Por razones de seguridad nacional y de eficacia de la acción externa del Estado, se considera

reservada aquella cuya revelación originaría un riesgo a la seguridad e integridad territorial del Estado y la defensa nacional en el ámbito externo, al curso de las negociaciones internacionales y/o la subsistencia del sistema democrático.

Esto incluye a los elementos de las negociaciones internacionales que de revelarse perjudicarían los procesos negociadores o alterarían los acuerdos adoptados (por lo tanto, no serán públicos al menos durante el curso de las mismas); información que al ser divulgada oficialmente por el Ministerio de Relaciones Exteriores pudiera afectar negativamente las relaciones diplomáticas con otros países; información oficial referida al tratamiento en el frente externo de la información clasificada en el ámbito militar; y los contratos de asesoría financiera o legal para realizar operaciones de endeudamiento público o administración de deuda del Gobierno Nacional; que de revelarse, perjudicarían o alterarían los mercados financieros (por lo tanto, no serán públicos por lo menos hasta que se concreten estas operaciones).

En estos casos, la regla general es un plazo de clasificación de cinco años con posibilidad de prórroga, salvo la información que encaja en la legislación de inteligencia (DL 1141), la cual es clasificada por 20 años prorrogables.

2.3. Información confidencial

Finalmente, en el tercer nivel de excepciones se encuentra la información confidencial. Esta abarca los siguientes supuestos:

- Documentos relativos al proceso de toma de decisiones: información que contenga consejos, recomendaciones u opiniones producidas como parte del proceso deliberativo y consultivo previo a la toma de una decisión de gobierno, salvo que dicha información sea pública. La excepción cesa si la decisión es adoptada siguiendo estos consejos u opiniones.
- Información protegida por el secreto bancario, tributario, comercial, industrial, tecnológico y bursátil. Es de aplicación el artículo 2.5 de la Constitución y la legislación especial en las diversas materias.
- Información vinculada a investigaciones en trámite referidas

al ejercicio de la potestad sancionadora de la Administración Pública. En este caso, la exclusión del acceso termina cuando la resolución que pone fin al procedimiento queda consentida o cuando transcurren más de seis (6) meses desde que se inició el procedimiento administrativo sancionador, sin que se haya dictado resolución final.

- Información preparada u obtenida por asesores jurídicos o abogados de las entidades públicas, cuando su difusión pudiera revelar la estrategia a adoptarse en la tramitación o defensa en un proceso administrativo o judicial, o de cualquier tipo de información protegida por el secreto profesional que debe guardar el abogado respecto de su asesorado. Esta excepción termina al concluir el proceso.
- Información referida a los datos personales cuya publicidad constituya una invasión de la intimidad personal y familiar, incluyendo aquella referida a la salud personal. En este caso, sólo el juez puede ordenar la publicación sin perjuicio de lo establecido en el artículo 2.5 de la Constitución.
- Aquellas materias cuyo acceso esté expresamente exceptuado por la Constitución o por una Ley aprobada por el Congreso.

2.4. Interpretación y aplicación de las excepciones

Como se ha explicado previamente, las excepciones al derecho de acceso a la información pública constituyen un *numerus clausus*: solo pueden invocarse en los supuestos taxativamente previstos por la ley. En consecuencia, su lectura debe ser restrictiva y siempre subordinada a la regla general de publicidad[12].

[12] Además, es importante considerar la doctrina jurisprudencial del Tribunal Constitucional. Así, por ejemplo, recientemente el Tribunal emitió cuatro criterios según los cuales no constituye información pública: (i) los borradores, textos o notas en desarrollo, apuntes preliminares o similares; (ii) los borradores, textos o notas en desarrollo, apuntes preliminares, actas, audios y videos, así como opiniones jurídicas especializadas no vinculantes o similares, utilizados en el proceso deliberativo de los órganos unipersonales o colegiados que administran justicia y

Al respecto, la Autoridad Nacional en materia de transparencia y acceso a la información pública ha señalado que en todos los casos, las excepciones deben leerse considerando el daño cierto, real o inminente, a los bienes jurídicos que recogen los artículos 15, 16 y 17: es decir, la seguridad nacional, la seguridad de las personas, la integridad territorial y/o la subsistencia del sistema democrático.

Asimismo, la misma Autoridad ha precisado que el daño real e inminente por la revelación de la información tiene que ser mayor al daño del interés público por conocer la información. Por ello, la interpretación de excepciones debe ser restringida y su aplicación solo debe permitirse en los casos expresamente establecidos en la norma. En ese sentido, al denegar el acceso a la información, la entidad debe fundamentar adecuadamente cuál de las causales reguladas es de aplicación, señalando de manera expresa las razones y el plazo por los que se aplica[13].

En el mismo sentido, el Tribunal Constitucional, en el caso Arellano Serquén, señaló que constituye una obligación de la entidad pública probar que (i) existe un apremiante interés público por mantener en reserva o secreto la información pública solicitada, y que (ii) tal reserva sirve efectivamente al interés público que le da cobertura[14].

Como se aprecia, para aplicar algunas de las excepciones revisadas en esta sección, no basta con mencionarla. Es necesario identificar cuál de ellas es de aplicación y verificar que *también* exista un daño real o inminente asociado a ella hacia la seguridad nacional,

---

del Ministerio Público; (iii) los correos electrónicos institucionales proporcionados por el Estado a sus funcionarios y servidores públicos, cuando el contenido de los mensajes almacenados no sea de carácter oficial; y (iv) os números telefónicos de celulares de uso personal, ni los entregados por la entidad para la que labora el funcionario o servidor público, así como la placa de rodaje de los vehículos de las entidades públicas, mientras dure su uso oficial por el usuario. Lamentablemente, la redacción de estas reglas es ambigua y de amplia interpretación, alcanzando a supuestos que sí constituyen información pública o que sí es posible transparentar. Ver sentencia recaída en el Exp. 04106-2022-PHD/TC.

13 Opinión consultiva 25 -2019-JUS/DGTAIPD.

14 STC Expediente N° 2579-2003-HD/TC Lambayeque, fundamento jurídico 6. Disponible en: https://www.tc.gob.pe/jurisprudencia/2004/02579-2003-HD%20Aclaracion.pdf

la seguridad de las personas, la integridad territorial y/o la subsistencia del sistema democrático. Todo ello debe ser fundamentado y explicado por el funcionario al momento de denegar el acceso a la información.

3. PROCEDIMIENTO PARA CLASIFICAR LA INFORMACIÓN

No existen definiciones propiamente dichas para los tres niveles de información clasificada (secreta, reservada y confidencial). Lo que sí hay es una lista cerrada de supuestos, revisados anteriormente, que nos permiten darle contenido y poder distinguir entre los tres tipos de clasificación. Además, cada uno de estos niveles corresponden a sectores distintos (defensa, orden interno, relaciones exteriores, etc.), y tienen asociadas obligaciones diferenciadas, como se verá a continuación.

La principal distinción es la relacionada con la clasificación. Se denomina "clasificación" al procedimiento o conjunto de acciones que realizan los funcionarios para establecer que determinada información se encuentra en algunos de los supuestos de exclusión del acceso[15]. La norma exige una formalidad diferenciada para este procedimiento, dependiendo de si se trata de información secreta, reservada o confidencial.

Para clasificar la información secreta y reservada, el procedimiento indica que el titular del sector o pliego —o quienes haya designado— son responsables de la clasificación que recae en los supuestos del artículo 15 y 16 de la Ley[16]. Ellos están a cargo de emitir una resolución que clasifique la información como secreta o reservada.

Esta resolución no contiene por sí misma información restringida. En consecuencia, su naturaleza es pública y puede ser entregada a cualquier ciudadano que la solicite, más allá de la obligación legal

[15] Opinión Consultiva 14-2020-JUS/DGTAIPD.

[16] Artículo 1 del Reglamento de la Ley, aprobado por Decreto Supremo 007-2024-JUS. Disponible en: https://cdn.www.gob.pe/uploads/document/file/6372106/5590378-decreto-supremo-que-aprueba-el-reglamento-de-la-ley-de-transparencia-y-acceso-a-la-informacion-publica.pdf?v=1716226343

que pueda existir para su publicación[17].

Asimismo, la norma prevé que l**as entidades que produzcan o posean información secreta y reservada deben contar con un registro de ella**[18]. En dicho registro, deben consignarse los siguientes datos: (i) el número y fecha de la resolución de clasificación; (ii) el número y fecha de resolución que designa al funcionario responsable de la clasificación, cuando sea el caso; (iii) el nombre o la denominación asignada, así como el código que se da a la información con el objeto de proteger su contenido, el mismo que debe estar consignado en el documento protegido; (iv) la fecha y resolución por la que se prorroga la clasificación; (v) el número, tipo de documento y la fecha con que se fundamenta ante el Consejo de Ministros el mantenimiento del carácter restringido de la información, cuando ello corresponda. Es importante resaltar que este registro tiene naturaleza pública y las entidades deben disponer su publicación en el Portal de Transparencia Estándar.

Este procedimiento **no está previsto para el caso de la información confidencial**, conforme indica el Reglamento. Es el funcionario poseedor de la información el que evalúa su naturaleza. Este funcionario no necesariamente debe tener competencia para emitir resoluciones —a diferencia del procedimiento para la información secreta y reservada, en la que la clasificación está a cargo del titular del pliego o sector, o quien designe—.

El reglamento establece, además, que las entidades pueden desarrollar procedimientos y/o emitir directivas internas que orienten la labor del funcionario responsable del área poseedora de evaluar la confidencialidad de la información. Estas directivas no deben contravenir las disposiciones reguladas en la normativa de transparencia y acceso a la información pública[19].

Finalmente, es importante resaltar que, al denegar una solicitud de acceso a la información pública por contener información reservada o secreta, las entidades deberán motivar su denegatoria acreditándola necesariamente con (i) la resolución que clasifica

17 Opinión Consultiva N° 13-2023-JUS/DGTAIPD

18 Artículo 39 del Reglamento.

19 Artículo 40 del Reglamento.

dicha información, la cual debe estar debidamente suscrita por el titular del pliego o la persona designada, y (ii) el registro de dicha información para el tratamiento correspondiente al interior de la entidad[20].

4. TENSIÓN ENTRE EL APARATO DE SEGURIDAD Y LA TRANSPARENCIA

La revisión del marco normativo revela que la mayor parte de las excepciones al derecho de acceso a la información pública está directamente vinculada con el aparato de seguridad del Estado: defensa nacional, relaciones exteriores, policía e inteligencia. Estos sectores concentran una proporción significativa de la información considerada "sensible" y, por tanto, clasificada. En la práctica, esta concentración genera un campo especialmente opaco, donde la regla general de publicidad cede terreno frente a la lógica de confidencialidad.

A esta opacidad se suma un régimen especial para la inteligencia, con plazos de reserva notablemente más extensos que en otros ámbitos. La propia Ley de Inteligencia refuerza esta dinámica al definir la información clasificada de inteligencia como aquella que los componentes del Sistema de Inteligencia Nacional (SINA) poseen o generan y que, por su naturaleza y contenido, "constituye una excepción al acceso público de conformidad con lo establecido en la Ley de Transparencia". Esta redacción introduce una circularidad preocupante: se restringe la información porque es clasificada, y es clasificada porque la ley permite restringirla.

El panorama se complejiza cuando se observan prácticas institucionales que revelan una débil cultura de transparencia. En 2022, por ejemplo, la Policía Nacional del Perú solicitó una opinión consultiva a la Autoridad Nacional de Transparencia para saber si estaba obligada como entidad por la Ley de Transparencia y Acceso a la Información Pública. La respuesta fue clara: "La ausencia de autonomía y de personalidad jurídica de una entidad de la Admi-

[20] Lineamientos Resolutivos II del Tribunal de Transparencia y Acceso a la Información Pública, aprobados por Resolución de Sala Plena N.° 000001-2022-SP.

nistración Pública no es óbice para ser reconocida como tal y ser considerada sujeto obligado por la normativa"[21]. Que una de las instituciones con mayores facultades de vigilancia haya necesitado esta aclaración ilustra no solo la falta de familiaridad con el marco legal, sino también un sistema que busca eludir en la medida de lo posible el principio de publicidad y la aplicación de las máximas garantías del marco de transparencia.

Incluso, en materia de defensa, en 2012, el Presidente de la República emitió un Decreto Legislativo por el cual se consideraba que toda información o documentación que se genere en el ámbito de los asuntos referidos a la Seguridad y Defensa Nacional, y las que contengan las deliberaciones sostenidas en las sesiones del Consejo de Seguridad y Defensa Nacional, era de carácter secreto[22]. Aunque esto luego fue modificado y se estableció que esta información se regía por la legislación de transparencia "en cuanto resulte aplicable", fue necesario un pronunciamiento del Tribunal Constitucional[23] para declarar como inconstitucional dicha formulación, pues no es discreción del Consejo decidir cuándo se aplica la legislación de transparencia y cuándo no. Si bien se logró corregir la redacción de la norma, la intención original de mantener cierta información fuera del escrutinio público es evidente.

En conjunto, este diseño normativo e institucional produce un ecosistema donde las facultades de vigilancia y control ejercidas por el aparato de seguridad están acompañadas de un blindaje legal robusto frente al escrutinio ciudadano. El resultado es un desequilibrio estructural: mientras las atribuciones para intervenir comunicaciones y acceder a datos se amplían, las posibilidades de la ciudadanía de conocer cómo, cuándo y con qué límites se ejercen esas facultades se reducen de manera drástica. El sistema, así configurado, parece construido para que sea muy poco lo que sabemos sobre estos sectores.

---

21 Opinión Consultiva 023-2022-JUS/DGTAIPD.

22 Decreto Legislativo 1129. Disponible en: https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H1068698

23 STC Expediente 0005-2013-PI/TC (2018). Disponible en: https://static.legis.pe/wp-content/uploads/2018/07/Expediente-00005-2013-PI-TC-Legis.pe_.pdf

CAPÍTULO 4: MISIÓN IMPOSIBLE: TRANSPARENTAR LA VIGILANCIA ESTATAL

1. LA CLÁUSULA DE SEGURIDAD NACIONAL

La noción de seguridad nacional no es de fácil definición. No obstante, hay múltiples referencias a ella en la ley y la Constitución. Como se ha revisado en el anterior capítulo, forma parte del núcleo normativo destinado al control del acceso a la información, apareciendo en en las leyes de transparencia e inteligencia, y operando como un "escudo" frente a la publicidad estatal.

En el Libro Blanco de la Defensa Nacional, elaborado por el Ministerio de Defensa[1], la seguridad es definida como aquella "situación en la cual el Estado tiene garantizada su independencia, soberanía e integridad y, la población los derechos fundamentales establecidos en la Constitución". Esa definición está presente también en la Política Nacional Multisectorial de Seguridad y Defensa Nacional al 2030 (PNMSDN)[2], y es coherente con la finalidad del Sistema de Defensa Na-

[1] Texto aprobado en la Octava sesión del Consejo de Seguridad Nacional (14 de abril de 2005). Su elaboración por parte del Ministerio de Defensa fue dispuesta mediante Decreto Supremo Nº 009/SG.

[2] Ministerio de Defensa (2022). Política Nacional Multisectorial de Seguridad y Defensa Nacional al 2030. Disponible en: https://cdn.www.gob.pe/

cional, según lo regulado por Decreto Legislativo 1129: "garantizar la seguridad nacional para la afirmación de los derechos fundamentales y el Estado constitucional de derecho, en el marco de una gestión pública moderna"[3].

Como se aprecia, el concepto va más allá de la connotación tradicionalmente militar que se le atribuye, e, incluso, trasciende a temas como la lucha contra el crimen. De hecho, la propia PNMSDN incluye lineamientos como asegurar la gobernabilidad del país, luchar contra la corrupción, promover la igualdad de oportunidades en áreas críticas, mejorar mecanismos de preservación del ambiente o promover el desarrollo de actividades en ciencia y tecnología en función de las necesidades de seguridad y defensa.

Sin embargo, la amplitud del término tiene implicaciones preocupantes al considerar que constituye el fundamento de las principales excepciones en el acceso a la información pública. De manera transversal,

> la tradición ligada a los estudios de seguridad nacional asume implícitamente que la apertura de información puede ser una debilidad que mine el funcionamiento de sus agencias y corporaciones. Se asume que la apertura y la desclasificación sólo beneficia a los enemigos internos o externos del país. La posición extrema de los defensores de este planteamiento parte del supuesto de que toda la materia de trabajo de esas organizaciones es secreta y no puede ser de otra forma[4].

Por supuesto, una de las características históricas de la actuación de las instituciones de seguridad y defensa fue su marcada opaci-

---

uploads/document/file/3350044/RESUMEN%20EJECUTIVO%20PNMSDN%20AL%202030.pdf.pdf?v=1656963441

[3] Artículo 2 del Decreto Legislativo 1129. Disponible en: https://cdn.www.gob.pe/uploads/document/file/1914632/DECRETO%20LEGISLATIVO%201129%20REGULA%20SISTEMA%20DE%20DEFENSA%20NACIONAL%20%281%29.pdf.pdf?v=1622134708

[4] Curzio Gutierres, Leonardo (2011). "Seguridad nacional y transparencia". *Transparencia focalizada. Ejercicio del derecho a la información pública en México*, p. 29. Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/12/5670/4.pdf

dad[5]. La experiencia autoritaria en América Latina demostró que la reserva absoluta no garantizaba más seguridad, sino más abusos. Precisamente, la superación de los modelos políticos autoritarios y el surgimiento de pactos democráticos —en particular, en el contexto de la post Guerra Fría— son los que dan lugar a una idea robusta de transparencia y rendición de cuentas, motivada por la necesidad de develar la actuación de los cuerpos de seguridad y las agencias de inteligencia para conocer su función en favor de estos regímenes totalitarios y autoritarios[6].

Sin embargo, esto no ha logrado irradiarse, precisamente, en lo que respecta al aparato de seguridad y defensa. Desde una perspectiva crítica, este uso extensivo y poco delimitado de la seguridad nacional configura un tipo de "securitización": se declara un asunto como una amenaza existencial, desplazándolo del debate democrático hacia un ámbito donde se justifican medidas extraordinarias sin el escrutinio público adecuado.

Así, se deja de lado la posibilidad de que la seguridad se incremente a partir de la publicidad de su información —en lugar de su reserva—. Diversas situaciones de riesgo pueden ser mejor manejadas cuando la ciudadanía tiene un mayor nivel de acceso a datos oficiales, documentados y confiables que den cuenta de las decisiones políticas. La apertura, en estos casos, no debilita al Estado, sino que lo fortalece al generar confianza pública y legitimidad. Evidentemente, esto no significa que no haya aspectos de seguridad que deban permanecer en reserva; sin embargo, esta reserva no puede extenderse de modo tal que estos sectores constituyan áreas completamente oscuras e inaccesibles al control ciudadano, especialmente cuando pueden representar una amenaza a grupos en situación de vulnerabilidad, como defensores de derechos humanos y periodistas.

Tal como ha se ha repasado en el capítulo anterior, las excepciones al derecho de acceso deben ser interpretadas de forma estricta y

[5] Magaloni Kerpel, Ana Laura (2011). "Transparencia focalizada en las instituciones federales de seguridad y persecución criminal". Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/12/5670/6.pdf

[6] Roberts Aldasair (2007), "Transparency in the security sector", The Right to know - transparency for an open world.

no expansiva. De lo contrario, la cláusula de seguridad nacional se convierte en una fórmula vacía y circular que justifica la opacidad, debilitando precisamente los principios de transparencia y rendición de cuentas que sostienen a un Estado democrático.

2. PRÁCTICAS DE VIGILANCIA ESTATAL EN EL PERÚ

La historia reciente de la vigilancia en el Perú está atravesada por episodios de secretismo, abuso político y adquisiciones tecnológicas opacas. Durante los años noventa, bajo el régimen de Alberto Fujimori, el entonces Servicio Nacional de Inteligencia (SIN) estuvo en el centro de múltiples denuncias por interceptaciones ilegales de comunicaciones y seguimiento político. Con la caída del régimen en el año 2000, se esperaba que estas prácticas desaparecieran junto con el aparato de inteligencia fujimorista. Sin embargo, los especialistas y los equipos de interceptación no se desactivaron por completo, sino que continuaron operando bajo nuevas dependencias estatales[7].

Una de las primeras confirmaciones de esta continuidad apareció en 2011, cuando el periodista Óscar Castilla reveló el funcionamiento de "Constelación": un sistema de intervención de las comunicaciones que la División Antidrogas de la Policía Nacional (Dirandro) operaba con asistencia técnica y equipos proporcionados por la Drug Enforcement Administration (DEA) de Estados Unidos[8]. Este sistema, que había empezado a funcionar en 2009, se justificaba bajo la lucha contra el narcotráfico y el crimen organizado, pero demostró que la capacidad de interceptación del Estado seguía activa y expandiéndose.

El uso político de estas capacidades se hizo evidente en 2015, cuando medios de comunicación denunciaron que la DINI realiza-

[7] Morachimo, Miguel (2016). *Vigilancia Estatal de las Comunicaciones y Derechos Fundamentales en Perú*. Hiperderecho & EFF.

[8] Castilla, Óscar (2011). "Así funciona Constelación, el sistema de escucha telefónica de la Dirandro". Disponible en: https://elcomercio.pe/sociedad/lima/asi-funciona-constelacion-sistema-escucha-telefonica-dirandro-noticia-1341509/

ba operaciones de seguimiento y espionaje con fines estratégicos para el gobierno de turno, monitoreando a políticos, empresarios y periodistas[9]. Como se reveló ese año, en 2013 se ejecutaron más de 54 millones de soles en adquisiciones a proveedores del extranjero con cargo a los recursos especiales de la DINI. De ellos, cerca de 50 millones estuvieron destinados a la contratación de Verint Systems Ltd, dependencia israelí que vende equipos de interceptación y espionaje a gobiernos, conforme ha documentado Amnistía Internacional[10]. Otros proveedores fueron Consitrade LLC, por más de 3 millones de soles; Vsense Technologies, por más de 1.6 millones de soles; The Barther Group LLC, por más de 100 mil soles; y Crime Off, por 25 mil soles. Estas adquisiciones no pudieron ser auditadas ni siquiera por la Contraloría de la República, aunque un cuadro simple fue remitido a la Comisión de Inteligencia del Congreso por la presión del contexto.

La crisis derivada de estas revelaciones obligó a la Presidencia del Consejo de Ministros a anunciar la disolución de la DINI en febrero de ese año. Un mes más tarde, la indignación pública desembocó en la censura del gabinete liderado por Ana Jara, la primera censura ministerial en más de medio siglo[11].

Estos episodios no solo evidenciaron la fragilidad institucional del aparato de inteligencia peruano, sino también su volatilidad: en apenas 25 años se han sucedido 21 jefes de inteligencia nacional[12], una rotación que recuerda a la de los presidentes del Consejo de Ministros, con 36 en el mismo periodo.

9 Cuarto Poder (2015). "DINI: Nuevos documentos confirmarían seguimientos a Alan García y Keiko Fujimori". Disponible en: https://www.americatv.com.pe/cuarto-poder/dini-nuevos-documentos-confirmarian-seguimientos-alan-garcia-y-keiko-fujimori-noticia-22831

10 Amnistía Internacional (2021): "South Sudan: Rampant abusive surveillance by NSS instils climate of fear". Disponible en: https://www.amnesty.org/en/latest/news/2021/02/south-sudan-abusive-surveillance-by-national-security-service-climate-of-fear-2/. Ver también Amnistía Internacional (2021). "These Walls Have Ears: The chilling effect of surveillance in South Sudan". Disponible en: https://www.amnesty.org/zh-hans/wp-content/uploads/2022/10/AFR6535772021ENGLISH.pdf

11 Morachimo, Miguel (2016). *Vigilancia Estatal de las Comunicaciones y Derechos Fundamentales en Perú*. Hiperderecho & EFF.

12 Caretas (21 de enero de 2025). "DINI: Guerra de espías". Disponible en: https://caretas.pe/politica/dini-guerra-de-espias/

Los escándalos no se limitaron a las prácticas de espionaje, sino que también alcanzaron a la adquisición de nuevas tecnologías de vigilancia. Un caso emblemático fue el llamado Proyecto Pisco, también del gobierno de Ollanta Humala. Según las investigaciones fiscales, Humala habría intervenido directamente para facilitar la compra de un sistema de interceptación telefónica a la dependencia israelí Verint Systems, valorado en más de 22 millones de dólares. El sistema fue donado al Ministerio del Interior para uso de la Dirección de Inteligencia de la Policía Nacional, pero nunca llegó a entrar en funcionamiento.

Pese a ello, documentos obtenidos por Associated Press[13] revelaron el verdadero alcance de la tecnología adquirida: el sistema podía intervenir hasta 300 líneas en simultáneo y acceder a cualquier tipo de comunicación, incluyendo telefonía fija, celular y servicios de Internet como correos electrónicos, mensajería instantánea o llamadas VoIP. Además, incorporaba funciones de geolocalización y permitía interceptar sin necesidad de colaboración de las empresas de telecomunicaciones, al operar directamente sobre las señales. Si bien el Proyecto Pisco fue objeto de investigaciones de la Contraloría y del Congreso, el carácter reservado de estos procesos impidió conocer con claridad cuál fue su destino final[14].

El despliegue de sistemas de vigilancia e interceptación de las comunicaciones también ha tenido manifestaciones más recientes. Además de las modificaciones legales que flexibilizan las garantías abordados en el capítulo 2, el contexto de crisis política agudizado a fines de 2021, con las protestas en contra de la toma de poder por parte de Manuel Merino, también propició un clima de miedo, persecución e incertidumbre. Como se pudo documentar, diversos activistas y manifestantes políticos refirieron sentirse monitoreados, haber recibido amenazas o incluso percibir vigilancia en sus

13 Frank Bajak y Jack Gillum (2016). "Cuando el Gran Hermano vigila: el espionaje a ciudadanos en era digital". Disponible en https://www.elnuevoherald.com/noticias/mundo/article93337867.html. La nota original en inglés en Associated Press puede revisarse aquí: https://web.archive.org/web/20210109094212/https://apnews.com/article/736dd5c3aa644cd499d6f6da8b9e5974

14 Morachimo, Miguel (2016). "El sistema de espionaje de las comunicaciones que dejó Humala". Disponible en: https://hiperderecho.org/2016/08/proyecto-pisco-skylock-peru-verint

domicilios[15].

Una nueva oleada de interés en elevar este tipo de medidas fue propiciado por el incremento del crimen organizado, en particular, de casos de extorsión y homicidio a transportistas[16] en el segundo semestre de 2024. Esta situación crítica, en la que la inseguridad ciudadana alcanzó niveles que no se documentaban desde hace décadas, también propició que se legitimen narrativas que favorecen la vigilancia en desmedro del derecho a la privacidad o la libertad de expresión sin las debidas garantías.

Por un lado, el titular del Ministerio del Interior en ese entonces, Juan José Santiváñez, anunció la adquisición de equipos de geolocalización para luchar contra el delito de extorsión[17]. En una sesión convocada por el Congreso de la República en setiembre, Santiváñez también anunció diversas medidas para responder a la crisis, entre las que se encontraban (i) la habilitación de una nueva línea telefónica exclusiva para la atención de este delito; (ii) el despliegue del programa de apagón de celulares en coordinación con Osiptel, Reniec, Migraciones y el MTC; (iii) y la ampliación de accesos de geolocalización a 800 efectivos policiales (cuando, antes de eso, eran 37). Con ello, 800 efectivos de la PNP tendrían acceso directo a la ubicación de todos los celulares a nivel nacional[18].

Poco después, la Presidenta de la República aprobó dos Transferencias de Partidas en el Presupuesto. La primera de ellas, aprobada el 14 de setiembre[19], se realizó a favor de la DINI por un monto total de 30 millones de soles en "actividades de inteligencia y contrainteligencia", para financiar "gastos asociados a la lucha contra la delincuencia y el crimen organizado, que incluye además el control,

15 Entrevistas realizadas por el equipo de Hiperderecho..

16 Puede encontrarse mayor información aquí: https://es.wikipedia.org/wiki/Crisis_de_extorsiones_al_transporte_p%C3%BAblico_en_el_Per%C3%BA

17 El Peruano. "PNP adquirirá equipos de geolocalización para luchar contra el delito de extorsión". Disponible en: https://elperuano.pe/noticia/250958-pnp-adquirira-

18 Las declaraciones pueden encontrarse en la transmisión en vivo de la sesión: https://www.facebook.com/share/v/WnTMNRRxX91MouNb/

19 Decreto Supremo 168-2024-EF, Decreto Supremo que autoriza una Transferencia de Partidas en el Presupuesto del Sector Público para el Año Fiscal 2024 a favor de la Dirección Nacional de Inteligencia. Disponible en: https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H1385184

investigación y sanción de dichas acciones". Si esta primera descripción es extraña, pues el sector de inteligencia no realiza actividades comunes de lucha contra la criminalidad —ni mucho menos está a cargo de la investigación y sanción de estos delitos—, lo más raro es el uso que se le habría estado dando a este presupuesto.

Según reportó el equipo de investigación del medio Perú21, las compras de equipos de inteligencia y de espionaje incluyen la adquisición de licencias de "Cyabra", un sistema que se instala en computadoras y que permite descubrir cuentas falsas en las redes sociales, ofrecer alertas, sistematizar las interacciones de "trolls" digitales y, en resumen, detectar ataques maliciosos contra actores gubernamentales. Además, también se contrataron los sistemas "Voyager", que emplea fuentes abiertas (es decir, se trata de una herramienta OSINT[20]) para descubrir conexiones sociales y monitoreo de comportamiento, y "FUSION", también OSINT.

La segunda transferencia de recursos se aprobó en favor del Ministerio del Interior el 30 de septiembre de 2024[21]. Esta transferencia de partidas ascendió a 14 millones de soles "para financiar gastos asociados a la lucha contra la delincuencia y el crimen organizado, que incluye además el control, investigación y sanción de dichas acciones" —es decir, con el mismo objeto que la transferencia autorizada hacia la DINI—. Las actividades comprendidas en esta transferencia son (i) desarrollo de acciones de carácter reservado; (ii) Inteligencia y Contrainteligencia; (iii) vigilancia policial de naturaleza civil; y (iv) mejora de los servicios del sistema de justicia penal, en específico, en cuanto a la investigación policial por la presunta comisión de un delito.

Aunque no hay información disponible sobre cómo se está empleando este presupuesto, se sabe que las adquisiciones en materia de equipos de vigilancia continúan. Por ejemplo, el siguiente Ministro del Interior Julio Diaz Zulueta, durante la II Reunión de Comando Policial (Recopol) celebrada en marzo de 2025 en Tarapoto, informó como uno de sus ejes de gestión el fortalecimiento de la

20 "Open Source Intelligence", en inglés.

21 Decreto Supremo 179-2024-EF. Disponible en: https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H1386050

inteligencia operativa. Para ello, anunció la compra de 4 maletines de geolocalización y un software de extracción de datos de celulares para la Policía Nacional[22].

Resulta cuestionable, además, que esta agenda se haya trasladado también a nivel de gobiernos regionales y locales. Es el caso de la Municipalidad Metropolitana de Lima, la cual cuenta con un Grupo Especial de Inteligencia Municipal (GEIM), creado en el primer trimestre de 2025. Aunque no quedan claras sus funciones, el propio alcalde López Aliaga ha declarado que el Grupo está a cargo de "chuponear" —esto es, interceptar— líneas telefónicas de supuestos delincuentes[23], a pesar de que por ningún motivo existe una habilitación legal que permita a las municipalidad realizar este tipo de operaciones.

El jefe de equipo, José Baella, ex general de la Dircote (Dirección contra el Terrorismo) y ex jefe de inteligencia de la PNP, señaló además que no se encuentran bajó ninguna supervisión, y que el detalle de identidad de los miembros del equipo es *reservado*. Lo único que reveló es que operan un software (sin mencionar cuál) que emplea fuentes abiertas y gubernamentales internas para la identificación de extorsionadores a partir de denuncias ciudadanas.

Por su parte, la Presidenta de la República hizo mención particular a la agenda de lucha contra la criminalidad en múltiples oportunidades durante su Mensaje a la Nación[24] del 28 de julio de 2025, como se realiza anualmente. Sin embargo, los datos brindados son bastante vagos. Así, por ejemplo, mencionó que se intensificaron las acciones de la PNP con "mayor equipamiento logístico y tecnológico", sin mayor especificación. En lo que respecta a la modernización tecnológica de la PNP, señaló que se han instalado "cámaras

22 Ver nota en: https://www.gob.pe/institucion/mininter/noticias/1137422-ministro-diaz-el-gobierno-esta-plenamente-enfocado-en-fortalecer-la-operatividad-e-inteligencia-en-la-pnp

23 Perú21 (marzo de 2025). "El servicio secreto de López Aliaga". Disponible en: https://peru21.pe/investigacion/lopez-aliaga-el-servicio-secreto-del-alcalde-de-lima-chuponeo/

24 Puede revisarse el Mensaje presidencial aquí: https://img.lpderecho.pe/wp-content/uploads/2025/07/Discurso-presidencial-Dina-Boluarte-2025-LP-derecho.pdf

de videovigilancia con inteligencia artificial", y que se está próximo a implementar un "sistema de videovigilancia inteligente con integración de 2480 cámaras a nivel nacional con licencias de inteligencia artificial", con una inversión mayor a 86 millones de soles. Por supuesto, no existe mayor información disponible sobre estos sistemas a la fecha de cierre de este informe.

3. CASOS OPACOS

La situación de vigilancia a través de las tecnologías en el Perú tiene diversas manifestaciones, conforme se ha revisado en el acápite anterior. Sin embargo, son muchas más las preguntas que las respuestas existentes respecto a su despliegue. A continuación se presentan algunos casos puntuales de secretismo y poca transparencia de los últimos años. Todos representan información que no está disponible para la ciudadanía en general; si bien algunos son de información clasificada en respuesta a solicitudes de acceso a la información pública presentados por el equipo legal Hiperderecho, otros constituyen denegatorias de acceso no justificadas en las excepciones legales revisadas en el capítulo 3, y otros representan la ausencia de protocolos para actividades de vigilancia que están amparadas por ley.

3.1. Protocolo de geolocalización

Conforme fue revisado en el capítulo 2, sección 1.2, la Policía Nacional del Perú puede acceder a la geolocalización de las personas sin contar con una orden judicial previa. Al amparo del Decreto Legislativo 1182 y sus modificatorias, el requerimiento fiscal y la convalidación del juez es posterior a la ejecución de la medida.

En octubre de 2015, mediante Resolución Ministerial 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", el cual establece las etapas del procedimiento del DL 1182. No obstante, el Ministerio clasificó este protocolo con el carácter de "reservado", atendiendo a la excepción de seguridad nacional prevista en la Ley de Transparencia y

Acceso a la Información Pública.

En consecuencia, ninguna persona tiene una idea clara sobre cuáles son los pasos seguidos por la PNP para acceder a información de geolocalización, ni mucho menos si es que se han previsto salvaguardas.

3.2. Ejecución de recursos transferidos al Ministerio del Interior

Conforme se exploró en la sección 2 de este capítulo, en septiembre de 2024 se aprobó una transferencia de recursos al Ministerio del Interior mediante Decreto Supremo 179-2024-EF[25], para actividades de inteligencia y contrainteligencia, vigilancia, investigación del delito y otros de carácter reservado (identificadas por los códigos de actividad presupuestal 5000889, 500128, 5004397 y 5000642, respectivamente). Desde su formulación, uno de los tipos de actividades autorizadas de esta transferencia es de acceso restringido a la ciudadanía, al tratarse, nominalmente, de "desarrollo de acciones de carácter reservado".

Para el resto de actividades, Hiperderecho presentó una solicitud de acceso a la información pública requiriendo el detalle de los posibles equipos tecnológicos, softwares, sistemas de información u otros bienes y servicios tecnológicos adquiridos, contratados o planificados con cargo a los recursos asignados en dicho decreto supremo, precisando:

- Nombre del bien o servicio (software, equipo, sistema, plataforma, etc.)
- Marca, modelo y especificaciones técnicas
- Finalidad o uso previsto (vigilancia, análisis, almacenamiento, monitoreo, etc.)
- Dependencia o unidad responsable de su gestión o uso
- Nombre del proveedor
- Monto del contrato

[25] Disponible en: https://cdn.www.gob.pe/uploads/document/file/7024222/6049192-ds179_2024ef.pdf?v=1727807811

Asimismo, también se solicitaron las copias de las resoluciones que autorizan o aprueban cada una de estas adquisiciones o contrataciones, así como los documentos de sustento disponibles (fichas técnicas, TDRs, contratos, convenios, etc.).

Para la atención de esta solicitud, el funcionario responsable de acceso a la información pública trasladó la consulta a la Oficina de Abastecimiento, quien la dirigió específicamente a la Coordinación de Ejecución Contractual (CEC). No obstante, dicha oficina respondió que el pedido no correspondía ser atendido por la CEC.

Además, señaló que el pedido "podría encontrarse dentro de algunas de las excepciones al ejercicio del derecho de acceso a la información contempladas en el TUO de la Ley N°27806, ya que, el numeral 1) del artículo 15 señala que la excepción al ejercicio del derecho al acceso a la información pública comprende únicamente los siguientes supuestos: "1. Información clasificada en el ámbito militar (y también policial), tanto en el frente interno como externo (...)", y complementando dicha información, el literal e) del numeral 1 del artículo 16° del TUO señala que constituye información reservada: e) "El armamento y material logístico comprendido en operaciones especiales y planes de seguridad y defensa del orden interno".

Este oficio fue remitido por el funcionario de transparencia a manera de respuesta, a pesar de que no responde a nada de lo solicitado. Por un lado, si la Coordinación de Ejecución Contractual consultada no posee la información, el requerimiento debe redirigirse a la oficina que sí la tenga, pues no es responsabilidad del administrado conocer qué dependencia interna la posee, ni mucho menos basta una negativa de alguna oficina para que se trate de una respuesta suficiente. De hecho, en ninguna parte de la respuesta se menciona que la entidad carezca de esos datos.

Por otro lado, tampoco es una respuesta suficiente, concluyente ni justificada la referencia a que *podría* ser información clasificada. Lamentablemente, el funcionario de transparencia únicamente tomó como respuesta lo señalado por el CEC sin hacer una evaluación del caso, ni dar una explicación clara del supuesto de excepción que, aparentemente, sería aplicable, junto con la justificación del daño en caso se divulgue dicha información y la copia

de resolución que la clasifica. Nada de esto fue considerado en la respuesta. En ese sentido, Hiperderecho presentó una apelación ante el Tribunal de Transparencia y Acceso a la Información Pública, aunque aún no hay una resolución de la misma.

En adición, al consultar en el Buscador Público del Sistema Electrónico de Contrataciones del Estado por procesos de selección que pudieran estar relacionados con esta transferencia presupuestaria. Así, se emplearon las palabras clave "vigilancia", "videovigilancia", "biometría", "inteligencia", "geolocalización", entre otros. Sin embargo, no hubo ningún resultado, lo cual indica que podrían tratarse de adquisiciones no escrutables públicamente al no haber pasado por los procesos de contratación regulares.

3.3. Protocolos de agentes virtuales

A fines de 2023, se ampliaron los agentes de las técnicas especiales de investigación. Así, al agente encubierto se le añadió, entre otros, la figura del agente virtual (ver sección 1.3 del Capítulo 1 para mayor claridad). No obstante, a la fecha no se sabe con exactitud cuál es su naturaleza ni sus ámbitos de actuación.

En ese sentido, Hiperderecho presentó una solicitud de acceso a la información pública requiriendo (i) los reglamentos, protocolos o cualquier otro documento que proporcione lineamientos para la actuación de agentes encubiertos y agentes virtuales; y (ii) los documentos de trabajo o cualquier otra coordinación entre la Secretaría de Gobierno y Transformación Digital y el MININTER para el desarrollo de protocolos, lineamientos o cualquier otro documento que guíe la actuación de agentes encubiertos en entornos digitales, conforme indica la segunda disposición complementaria final de la Ley 30096 (modificado por DL 1591).

En respuesta, la PNP señaló que la técnica especial de investigación denominada "agente encubierto" está regulada en el "Reglamento de Circulación y Entrega Vigilada Bienes Delictivos, Agente Encubierto y Operaciones Encubiertas", aprobado por Resolución

5321-2015-MP-FN de la Fiscalía de la Nación[26] en el año 2015. No obstante, no se ofreció ninguna respuesta con respecto a los protocolos de la técnica de "agente virtual", a pesar de que, precisamente, es la nueva figura creada en 2023, sobre la cual no se tiene mayor detalle ni información. En este caso, se trata de una respuesta incompleta que no satisface el derecho de acceso a la información pública, al no haber un pronunciamiento formal sobre ese extremo de la solicitud (ni siquiera para mencionar que la información no existe o no está en posesión de la entidad).

Por su parte, la Presidencia de Consejo de Ministros precisó que la Secretaría de Gobierno y Transformación Digital "realizó las acciones correspondientes a fin de recabar los datos personales de los puntos focales que participarían en una Mesa de Trabajo a fin de elaborar los protocolos para la actuación de agentes encubiertos en entornos digitales, información que trasladada al Ministerio Público – Fiscalía de la Nación con Oficio N° 001220-2024-PCM-SGTD de 15 de octubre del 2024, no obstante, hasta la fecha no se ha emitido ningún documento que guíe la actuación de agentes encubiertos en entornos digitales". Además, la Subsecretaría de Política y Regulación sugirió que cualquier documento que se genere luego de estas eventuales mesas o reuniones previas a la aprobación de algún protocolo debe ser tratado como información confidencial.

3.4. Información secreta de la DINI

Hiperderecho presentó una solicitud de acceso a la información pública a la DINI para que proporcione la lista de solicitudes de acceso a la información pública denegadas por tratarse de información clasificada como secreta entre 2020 y 2025, incluyendo las copias de las resoluciones que clasifican dicha información.

En respuesta, la DINI detalló la información requerida en estas solicitudes que fueron eventualmente denegadas. Entre ellas destacan las siguientes:

[26] Disponible en: https://portal.mpfn.gob.pe/descargas/ncpp/files/7475f8_RFN-5321-2015-MP-FN-Reglamento-de-Circulacion-compressed.pdf

- Nombres y apellidos completos de responsables del Libro de Reclamaciones (2021)
- Listado de planilla de asesores de la Alta Dirección de la DINI (2022)
- Informe de Inteligencia N° 028- 2022, mencionado por el Premier Aníbal Torres como justificación para la inmovilización obligatoria del 5 de abril de 2022 (2022)
- Directiva que regula contrataciones fuera del ámbito de Ley de Contrataciones (2022)
- Estado actual de proyecto "Pisco" (2023)
- Informe de transferencia y rendición de cuentas (2023)
- Amenazas a la Seguridad Nacional (2025)

Como se observa, los temas cubiertos por estas solicitudes van desde cuestiones administrativas de bajo perfil hasta documentos estratégicos de alto impacto político y social. El hecho de que informes que justificaron decisiones excepcionales de orden público, directivas sobre contrataciones y el estado del proyecto de interceptación "Pisco" se mantengan en reserva evidencia cómo la clasificación de información se aplica de manera amplia. En particular, la negativa a informar sobre Pisco —un sistema de vigilancia que ya ha sido ampliamente cuestionado en la opinión pública— muestra que incluso los proyectos más emblemáticos y polémicos en materia de interceptación continúan rodeados de opacidad, lo que limita el escrutinio ciudadano sobre el alcance real de las capacidades de vigilancia en el país.

3.5. Lista de excepciones para contrataciones directas secretas

En el Perú, los instrumentos normativos más importantes en materia de contrataciones públicas son la Ley 30225, Ley de Contrataciones del Estado[27], y su Reglamento[28], aprobado por Decreto Supremo 344-2018-EF.

[27] Disponible en: https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H1105713
[28] Disponible en: https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H1224904

Al amparo de esta Ley, se prevé el mecanismo excepcional de contrataciones directas —es decir, sin concurso público—, para lo cual las entidades cuentan con una lista limitada de supuestos detallados en el artículo 27. Entre ellos, se considera "cuando las Fuerzas Armadas, la Policía Nacional del Perú y los organismos conformantes del Sistema Nacional de Inteligencia requieran efectuar contrataciones con carácter secreto, secreto militar o por razones de orden interno, que deban mantenerse en reserva conforme a ley, previa opinión favorable de la Contraloría General de la República".

Esto es desarrollado posteriormente por el artículo 100 del Reglamento, según el cual las contrataciones directas con un proveedor pueden realizarse, entre otros supuestos, cuando se trate de contrataciones de carácter secreto, secreto militar o por razones de orden interno, las cuales:

> "Son aquellas cuyo objeto contractual se encuentra incluido en la lista que, mediante decreto supremo, haya aprobado el Consejo de Ministros, debidamente refrendado por el sector correspondiente. La presente causal no es aplicable a la contratación de bienes, servicios en general, consultorías u obras de carácter administrativo u operativo necesarios para el normal funcionamiento de las Fuerzas Armadas, la Policía Nacional del Perú y los organismos que conforman el Sistema de Inteligencia Nacional.
>
> La opinión favorable de la Contraloría General de la República se sustenta en la comprobación de la inclusión del objeto de la contratación en la lista a que se refiere el numeral anterior y se emite dentro del plazo de siete (7) días hábiles a partir de presentada la solicitud."

En otras palabras, para contrataciones directas de carácter secreto, es necesario que el Consejo de Ministros apruebe una lista previa que contiene los objetos contractuales pasibles de fundamentar este tipo de contrataciones.

Al respecto, Hiperderecho presentó una solicitud de acceso a la información pública para conocer el contenido de esta lista y cualquier otro documento relacionado con ella. No obstante, a pesar de que esta disposición reglamentaria existe desde 2018, la Presidencia de Consejo de Ministros manifestó que la información requerida *no existe,* por lo cual no se puede atender la solicitud. Asimismo, la Oficina de Asesoría Legal de la referida entidad añadió que "no se encuentra obligada a realizar un análisis de las normas

legales vigentes, para determinar la lista solicitada", al amparo de la Ley de Transparencia. En ese sentido, el pedido se denegó por inexistente.

No obstante, al haber evidencia documentada de adquisición de equipos y softwares de vigilancia, y al no existir información de convocatorias públicas en el SEACE, queda claro que se están realizando contrataciones directas haciendo uso de esta cláusula. La pregunta es cómo pueden concretarse sin cumplir con el requerimiento que plantea la propia norma.

3.6. Grupo de Inteligencia Municipal

Conforme se abordó en la sección 2 de este capítulo, en marzo de 2025 la Municipalidad Metropolitana de Lima anunció la creación del Grupo Especial de Inteligencia Municipal como respuesta a la crisis de extorsión actual. A partir de la información disponible del Organismo Especializado para las Contrataciones Públicas, se sabe que el jefe de dicho equipo, José Baella, fue contratado por órdenes de servicio entre octubre de 2024 hasta mayo de 2025 por 84 mil soles (es decir, 12 mil soles al mes).

En atención al secretismo alrededor del funcionamiento de este Grupo, Hiperderecho solicitó la siguiente información: (i) documentos sobre las funciones del GEIM y presupuesto asignado; (ii) informes sobre balance de actividades y logros alcanzados por el GEIM; (iii) contratos u órdenes de servicio del personal que integra el GEIM; (iv) boletas, recibos o informes sobre compra de software y/o dispositivos tecnológicos para las funciones del GEIM; y (v) documentos, cartas o e-mails que den cuenta de alianzas o colaboraciones entre el GEIM y otras instituciones públicas.

Al respecto, la Municipalidad respondió lo siguiente:

- **Funciones**: El GEIM tiene a su cargo la atención de llamadas telefónicas de ciudadanos que quieran realizar denuncias sobre delitos de extorsión y sicariato y, de corresponder, derivar a las unidades especializadas de investigación de la PNP en la región policial de Lima. También tienen a su cargo recibir reportes anónimos sobre personas requisitoriadas que permitan su identificación, ubicación y captura por parte de la PNP.

- **Logros**: Hasta abril de 2025, la Municipalidad reporta haber recibido 1307 llamadas a la línea habilitada (610-1010), de las cuales 164 (el 12%) han sido realizadas por personas víctimas del delito de extorsión. La información procesada se habría remitido a las unidades de investigación e inteligencia, para el inicio y orientación de investigaciones policiales.
- **Contratos u órdenes de servicio del personal**: Son 7 locadores de servicio integrando el GEIM. Por razones de seguridad, se guarda la reserva de sus identidades, aunque se refiere que sus órdenes de servicio son públicas en el portal de la OSCE.
- **Compra de software y/o dispositivos tecnológicos:** La Municipalidad señaló únicamente que "No corresponde informar".
- **Alianzas o colaboraciones con otras entidades:** La Municipalidad denegó este extremo del pedido por no considerarlo claro, al amparo del artículo 13, que señala como uno de los requisitos obligatorios de las solicitudes de acceso la "expresión concreta y precisa del pedido de información".

Al respecto, es necesario llamar la atención sobre dos puntos importantes. El primero es el relativo a la información sobre las órdenes de servicio: aunque se menciona que es información sobre la cual "se debe guardar reserva", no hay ninguna especificación sobre la aparente causal de clasificación; de hecho, ni siquiera se menciona que se está denegando esta información por ser clasificada. En adición, cuando la Municipalidad señala que las órdenes de servicio están publicadas en OSCE, se refiere al dataset de "órdenes de compra y órdenes de servicio", el cual constituye una lista mensual. En ella se pueden leer todos los proveedores y montos de contratación; sin embargo, no se expresa ni el número de convocatoria ni mucho menos sus detalles. En consecuencia, solo es una lista de todos los nombres de personas naturales o jurídicas contratadas mensualmente, pero no es posible saber cuáles de ellas, y por qué montos, corresponden al GEIM.

El segundo punto cuestionable es el relativo a la compra de software o dispositivos tecnológicos en el marco del GEIM. La Munici-

palidad, al responder escuetamente un "No corresponde informar", no da lugar a que el ciudadano conozca la razón por la cual se da respuesta al requerimiento. Esto también vulnera los principios del derecho de acceso a la información pública, pues, nuevamente, no se ofrece una respuesta concluyente. No se especifica si la información no existe, si no se han realizado compras, o si estas compras tienen carácter reservado o clasificado: simplemente, se deja el pedido sin atender. Esto es particularmente grave considerando el impacto que estas tecnologías pueden tener sobre los derechos de las personas, sobre todo en un contexto de opacidad en el que no se conoce cómo estarían siendo empleadas.

Esta respuesta ha sido apelada por Hiperderecho ante el Tribunal de Transparencia y Acceso a la Información Pública, aunque aún no se ha emitido una resolución de la misma ni se ha podido acceder a la información faltante.

3.7. Falta de transparencia activa

Aunque en la mayoría de este informe se ha hecho énfasis en la obligación de las entidades de dar respuesta a las solicitudes de acceso a la información pública presentadas por la ciudadanía, la transparencia en realidad abarca mucho más que eso. Esta dimensión pasiva, aunque importante, debe estar acompañada también de una transparencia activa: aquella que guía la publicación de información relevante por la propia entidad en sus portales institucionales —esto es, sin que sea necesario que la información sea solicitada—.

Un buen ejemplo de esta dimensión de la transparencia es el Portal de Transparencia Estándar con que debe contar toda entidad, el cual abarca cierta información clave obligatoria (por ejemplo, Manual de Organización y Funciones, presupuesto, información de funcionarios, etc.). En lo que respecta a esta investigación, este Portal también debe contener el registro de información secreta y reservada (en la cual se incluyen los números de resoluciones de clasificación, periodo de clasificación, etc.).

No obstante, de la revisión de los Portales de Transparencia Estándar de la DINI, Mininter y Mindef no se ha encontrado que exista información pública sobre el registro de información clasificada.

CONCLUSIONES Y RECOMENDACIONES

1. La vigilancia estatal, en tanto ejercicio de poder intrusivo, plantea riesgos evidentes para los derechos fundamentales, especialmente el derecho a la privacidad y la libertad de expresión. Cuando se afectan estos derechos mediante medidas como la intervención de comunicaciones o la recopilación de datos sin control ni garantías, se produce además un efecto inhibitorio: la existencia de un aparato de vigilancia puede desalentar la participación política, la crítica al poder o la organización colectiva; más aún cuando no se conoce cómo funciona. Por ello, la ejecución de estas medidas exige siempre requisitos claros, salvaguardas efectivas y mecanismos de control externo que aseguren su aplicación excepcional y justificada.

2. El derecho de acceso a la información pública en el Perú, a pesar de su reconocimiento constitucional, enfrenta serias restricciones cuando se trata del aparato de seguridad e inteligencia. La amplitud con la que se invoca la cláusula de seguridad nacional hace frágil el ejercicio de este derecho, a pesar de que la propia norma indica que estas excepciones deben interpretarse de manera restrictiva —lo cual, lamentablemente, no sucede así en la práctica—.

3. La revisión de las excepciones previstas en la legislación vigente muestra que la mayoría están diseñadas para blindar a sectores estratégicos del Estado —Defensa, Interior e Inteligencia— frente al escrutinio ciudadano. Aunque es claro que en todo Estado hay información que debe mantenerse restringida, lo cierto es que la seguridad nacional como concepto tiene amplios alcances que involucran incluso la identidad nacional o el equili-

brio ambiental. En ese sentido, no hay parámetros claros de la manera en que esta cláusula justifica la denegatoria de acceso a la información pública. Además, al restringir la transparencia precisamente en estos sectores, se deja de lado la importancia de incrementar la confianza ciudadana en estas instituciones, que son de las más desprestigiadas institucionalmente a nivel nacional.

4. La naturaleza circular de la definición de "información clasificada de inteligencia", presente en el Decreto Legislativo 1141, plantea problemas importantes. El Decreto refiere que es información clasificada de inteligencia aquella que constituya una excepción a la legislación de transparencia; sin embargo, no hay un parámetro claro sobre cómo identificarla y distinguirla de las demás excepciones comunes de la norma. Esto es más grave cuando se toma en cuenta que el periodo de clasificación es mucho mayor en el sector de inteligencia: son 20 años (versus los 5 años comunes de otro tipo de información).

5. Los hallazgos históricos y periodísticos confirman que la vigilancia estatal en el Perú no es un fenómeno nuevo ni aislado, sino parte de una práctica sostenida que atraviesa gobiernos de distinto signo político. Desde las operaciones del Servicio de Inteligencia Nacional en los noventa hasta la compra del sistema Voyager, la vigilancia ha sido ejercida con un patrón de secretismo y, en muchos casos, con cuestionamientos sobre su legalidad y legitimidad. La opacidad no solo protege las operaciones actuales, sino que también borra las huellas de posibles abusos pasados.

6. El examen de solicitudes de acceso a la información denegadas, en particular en el caso de la DINI, confirma que las excepciones se aplican de manera indiscriminada y desproporcionada. Documentos que, a primera

vista, carecen de relevancia estratégica para la seguridad nacional —como directivas administrativas o listados de planilla— son blindados con la misma severidad que informes de inteligencia sensibles. Esta práctica desnaturaliza el espíritu de la ley y erosiona la confianza ciudadana en la gestión pública. Incluso, los nombres de los funcionarios encargados de la Oficina de Transparencia son clasificados y no están publicados.

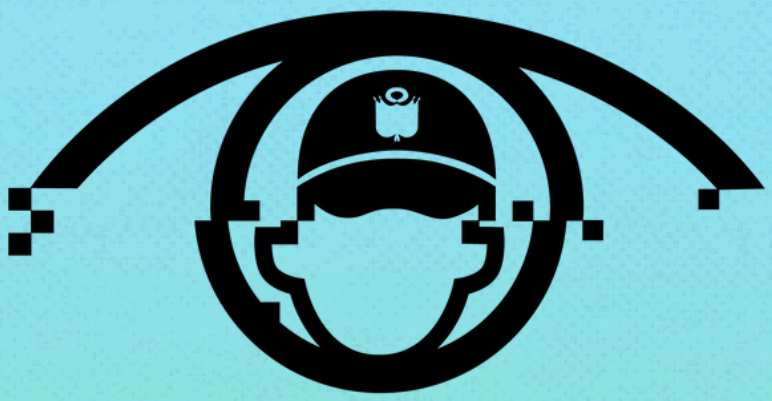
7. Más allá de la norma, el problema central es la pobre cultura de la transparencia que se ha enraizado en las instituciones peruanas. Los casos de denegación de información demuestran que las excepciones no son aplicadas con rigor, sino que a menudo se utilizan respuestas vagas y coloquiales como "no corresponde" o "esto podría ser clasificado". Esta práctica evidencia una falta de compromiso real con la transparencia tal como la ley la exige. El desfase institucional es tal que, hasta hace pocos años, la propia Policía Nacional del Perú dudaba de su condición de sujeto obligado por la Ley de Transparencia. Este hecho subraya que la resistencia a ser fiscalizado no es solo una cuestión normativa, sino un problema cultural y estructural que evidencia la falta de interiorización de los principios democráticos en entidades que ejercen un poder enorme sobre la vida de la ciudadanía.

8. Desde una perspectiva democrática, el actual diseño normativo coloca en tensión dos bienes jurídicos igualmente valiosos: la seguridad y la transparencia. Sin embargo, en la práctica, el primero se ha impuesto de forma casi absoluta sobre el segundo. Esta balanza desequilibrada ha permitido que la seguridad nacional opere como un argumento comodín que clausura el debate público, limitando la posibilidad de un escrutinio informado sobre cómo se ejercen las facultades más intrusivas del Estado.

9. De cara al futuro, resulta imprescindible replantear el marco normativo para incorporar mecanismos de control independiente sobre la clasificación de la información en materia de seguridad e inteligencia. No puede seguir siendo una potestad exclusiva de las propias entidades interesadas en mantener la reserva. La creación de órganos externos de supervisión, la participación activa de la Autoridad Nacional de Transparencia y un rol más robusto del Congreso en esta materia son pasos necesarios para equilibrar la balanza.

10. A lo anterior se debería sumar una reforma orientada a garantizar mayor protección frente a la arbitrariedad en el uso de la "confidencialidad" como categoría. Aunque no sucedió en el caso concreto, la Municipalidad de Lima fácilmente podría haber podido argumentar que la información solicitada era confidencial, y en ese caso ni siquiera se hubiera requerido que adjunte la resolución de clasificación.

11. También sería recomendable introducir innovaciones que reduzcan el costo político y social de solicitar información, como la posibilidad de realizar pedidos de acceso de manera anónima, con el fin de proteger a periodistas, activistas o personas investigadoras de posibles represalias. Precisamente, indagar en estos temas puede colocar a estos grupos en un mayor riesgo de ser vigilados, generándose un círculo vicioso: aquellas personas que desean mayor transparencia y rendición de cuentas sobre los mecanismos de vigilancia, posiblemente por considerarse expuestas a ellas, podrían convertirse en nuevos objetivos de seguimiento.



HIPERDERECHO