PODER PÚBLICO SIN HABILITACIÓN CONSTITUCIONAL

Software de espionaje y el marco legal de adquisición, transparencia e inteligencia en el Perú

HIPER DERE CHO

Dilmar Villena Fernández Baca

Poder público sin habilitación constitucional: Software de espionaje y el marco legal de adquisición, transparencia e inteligencia en el Perú ¿Es el spyware una tecnología legalmente viable en nuestro país?

Financiamiento
Esta es una publicación realizada dentro del marco del proyecto "Spyware under scrutiny: Research, incidence, and prevention within the Peruvian context", desarrollado por la asociación civil Hiperderecho. Agradecemos a New Venture Fund por financiar esta investigación.

Autoría
Dilmar Villena Fernández Baca

Revisión Legal
Lucía León Pacheco

Rubiela Gaspar

Diagramación
Lorena Marks

Ilustraciones de portada
Jugo gástrico

Diagramación de portada
Lorena Marks

Iconos
The Noun Project

Asociación Civil Hiperderecho
hola@hiperderecho.org

Algunos derechos reservados, mayo de 2026
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: LA VIGILANCIA Y EL SPYWARE EN EL CONTEXTO LEGAL PERUANO 7

1. La vigilancia estatal 8

1.1. Mecanismos generales de vigilancia estatal 10

a. Intervención de comunicaciones 10

b. Geolocalización 11

c. Monitoreo de redes sociales o ciberpatrullaje 11

d. Videovigilancia 12

e. Reconocimiento y/o identificación biométrica 12

1.2. El spyware como forma particularmente intrusiva de vigilancia digital 13

CAPÍTULO 1: DERECHOS FUNDAMENTALES EN TENSIÓN: IMPACTOS DIRECTOS E INDIRECTOS DEL SPYWARE 17

1. Derechos afectados de forma directa 18

1.1. Derecho a la vida privada e intimidad 18

1.2. Derecho a la protección de datos personales y/o autodeterminación informativa 19

1.3. Derecho al secreto e inviolabilidad de las comunicaciones 20

1.4. Derecho al debido proceso, derecho de defensa y licitud probatoria 21

1.5. Dignidad humana, autonomía personal y libre desarrollo 22

2. Derechos afectados de forma indirecta: el efecto inhibitorio 23

2.1. Libertad de expresión, opinión e información 23

2.2. Secreto profesional y protección de fuentes periodísticas 24

2.3. Libertad de reunión y derecho de asociación 25

2.4. Derecho a la integridad física, psíquica y moral 26

2.5. Libertad de pensamiento, conciencia y religión 27

CAPÍTULO 2: MARCO LEGAL DE LAS CONTRATACIONES DEL ESTADO PARA TECNOLOGÍAS DE VIGILANCIA (Y SPYWARE) 29

1. Régimen General de Contrataciones (Ley 32069) 29

1.1. Rol de los principios en el marco legal de contrataciones del estado 30

1.2. Principio de transparencia y principio de publicidad 31

2. Tipos de procedimientos de selección y mecanismos de control para el spyware 32

2.1. Los dos regímenes de contratación: procedimientos competitivos y no competitivos 33

2.2. Compra de spyware mediante procedimiento competitivo: publicidad, competencia y trazabilidad relativa 34

2.3. Procedimientos no competitivos: contratación directa y riesgo de opacidad 35

a) Proveedor único o derechos exclusivos 36

b) Contrataciones secretas de Fuerzas Armadas, PNP y SINA 38

3. Recapitulación: formas de adquisición de spyware por el Estado 40

CAPÍTULO 3: TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y SPYWARE 43

1. Principio de publicidad frente a cultura del secreto 43

2. Análisis de las excepciones en la Ley de Transparencia y Acceso a la Información Pública 45

2.1. Información secreta: ámbito militar e inteligencia 45

2.2. Información reservada: orden interno y criminalidad, y acción externa del Estado 47

2.3. Información confidencial: deliberación y s ecreto comercial 49

3. Interpretación restrictiva y violaciones a los derechos humanos 50
4. Plazos de clasificación: régimen común, régimen de inteligencia y problema de asimetría 51
5. Vigilancia y clasificación de información: qué no se podría clasificar 52

CAPÍTULO 4: SISTEMA DE INTELIGENCIA NACIONAL Y USO DE SPYWARE 54

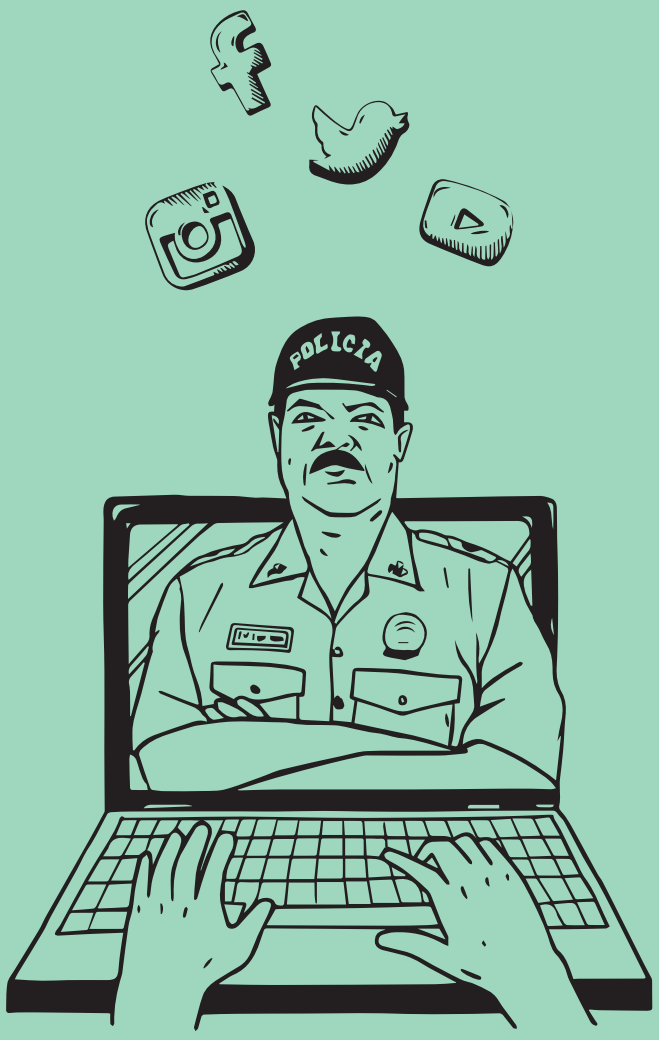
1. La inteligencia y el principio de legitimidad: seguridad nacional, derechos fundamentales y legalidad 54
2. Mecanismos de control de la actividad de inteligencia frente al uso de spyware 56
2.1. Control judicial 56
2.2. Valor probatorio de los informes de inteligencia y límites frente al proceso penal 58
2.3. Destrucción obligatoria de información innecesaria y derechos fundamentales 59
3. Recursos especiales y contrataciones reservadas: una zona de opacidad reforzada 60
4. Inteligencia y legalidad como requisito de clasificación de información legítima 61
5. Información de inteligencia sobre spyware que debería ser accesible 63

CAPÍTULO 5: ¿VIABILIDAD CONSTITUCIONAL DEL SPYWARE EN EL PERÚ? 64

1. La exigencia constitucional de orden judicial 65
2. Los dos únicos marcos normativos posibles: proceso penal e inteligencia 67

2.1. El artículo 230 del Código Procesal Penal: habilitación judicial, pero insuficiente para spyware 68
2.2. Procedimientos especiales de inteligencia 71
3. Spyware en el Perú: necesidad de moratoria y recomendaciones de política pública 73
3.1. Moratoria sobre la venta, transferencia y uso de tecnologías de spyware 73
3.2. Garantías mínimas para habilitar la adquisición y uso de spyware en Perú 77
3.2.1. Garantías de transparencia y publicidad 77
3.2.2. Mínimos respecto de proveedores 78
3.2.3. Legalidad y habilitación normativa explícita, taxativa y detallada 79
3.2.4. Autorización judicial 80
3.2.5. Garantías de ejecución técnica 81
3.2.6. Registro, trazabilidad y cadena de custodia 81
3.2.7. Notificación y recurso efectivo 82
3.2.8. Garantías frente a sujetos especialmente protegidos 82
3.2.9. Control independiente y auditoría 83
CONCLUSIONES 84

LA VIGILANCIA Y EL SPYWARE EN EL CONTEXTO LEGAL PERUANO



El presente informe parte de un presupuesto: la vigilancia no constituye un fenómeno exclusivamente estatal ni necesariamente ilegal, sino una práctica de observación, registro y análisis de actividades humanas que, con el desarrollo tecnológico, ha adquirido una intensidad inédita frente a los derechos de, entre otros, intimidad, privacidad y protección de datos personales. En efecto, como advierte León Pacheco[1], la vigilancia puede ser entendida como uno de los desafíos específicos que el desarrollo tecnológico plantea a la privacidad, en tanto permite observar y registrar actividades humanas mediante capacidades cada vez más sofisticadas de recolección, almacenamiento y análisis de información.

En esa línea, entendemos por vigilancia, en sentido general, al conjunto de prácticas, técnicas y tecnologías orientadas a observar, registrar, recolectar, procesar o analizar información sobre personas, grupos o comunidades, ya sea en espacios físicos, comunicacionales o digitales. Esta definición permite comprender que la vigilancia no se agota en la interceptación de comunicacio-

[1] León Pacheco, Lucía. *Vigilados en secreto: normas, prácticas y silencios en el acceso a información pública sobre vigilancia* (Lima: Hiperderecho, 2025).

nes, sino que comprende un ecosistema más amplio de extracción de información, producción de perfiles, seguimiento de conductas y análisis de patrones.

¿Dónde radica, entonces, la novedad del problema actual? No necesariamente en que la vigilancia exista, sino en la escala, persistencia y profundidad con la que puede desplegarse. En efecto, en el contexto del siglo XXI, las capacidades tecnológicas permiten a gobiernos y empresas interceptar, extraer, filtrar, almacenar y analizar comunicaciones privadas, huellas digitales y metadatos de comunidades enteras[2] y de forma sistemática. Así, la vigilancia contemporánea no se limita a mirar: permite reconstruir comportamientos, inferir vínculos, anticipar desplazamientos y producir conocimiento accionable sobre la vida privada de las personas.

1. LA VIGILANCIA ESTATAL

A continuación desarrollaremos una categoría más específica de vigilancia: la vigilancia estatal. Esta puede ser definida como el conjunto de actividades de monitoreo, interceptación, recolección, análisis, uso, preservación y retención de información sobre actividades, comunicaciones y datos de personas o colectividades, realizadas por entidades gubernamentales o por agentes del Estado[3].

Esta definición es importante porque desplaza el análisis del presente reporte de la mera capacidad técnica de vigilar hacia el problema jurídico del poder público (y sus posibles límites). Dicho de otro modo, cuando la vigilancia es realizada por el Estado, no estamos únicamente ante una tecnología de observación, sino ante una potestad pública que puede afectar derechos fundamentales y que, por tanto, debería contar con habilitación legal, finalidad legítima, necesidad, proporcionalidad, control independiente y mecanismos efectivos de rendición de cuentas.

---

2 Ídem.

3 Íbid.

En esta línea, podemos disgregar a la vigilancia estatal en, al menos, dos formas principales. En primer lugar, puede ser masiva, cuando implica la recolección de información a gran escala sobre una pluralidad amplia o indeterminada de personas. En segundo lugar, puede ser dirigida, cuando se orienta hacia personas, grupos, dispositivos o comunicaciones específicas bajo un esquema de monitoreo particular[4]. No obstante ello, esta distinción no siempre opera con nitidez cuando la vigilancia se realiza a través de tecnologías digitales o en entornos digitales, pues una medida formalmente dirigida hacia una persona específica puede terminar capturando información de terceros, redes de contacto, comunidades profesionales o entornos familiares completos: de esta forma, se borra el límite difuso entre vigilancia masiva y vigilancia dirigida.

Como ha advertido la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (en adelante, RELE), el uso estatal de tecnologías avanzadas de vigilancia digital supone una amenaza intensa para los derechos humanos, en tanto las arquitecturas estatales de cumplimiento del derecho internacional no han seguido el ritmo de los avances tecnológicos[5]. Además, ha observado que las repercusiones de la vigilancia digital no se agotan en la persona directamente afectada, sino que alcanzan a sus familias, contactos, medios de comunicación, espacios de participación pública y, en último término, a la democracia misma[6].

En el caso peruano, las actividades de vigilancia suelen justificarse jurídicamente bajo conceptos como la seguridad nacional, la prevención del delito, el mantenimiento del orden interno o la lucha contra el terrorismo[7]. Si bien tales finalidades pueden constituir objetivos constitucionalmente legítimos, su sola invocación no convierte en legítima cualquier medida de vigilancia. En efecto, y para mayor preocupación,

4 Íbid.

5 Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos. *El impacto de la vigilancia digital en la libertad de expresión en las Américas.* (OEA, 2025)

6 Íbidem.

7 León Pacheco, Lucía. Loc. Cit.

en la práctica institucional peruana, expresiones como "seguridad nacional" u "orden interno" pueden operar como categorías de cierre frente al escrutinio ciudadano, especialmente cuando se combinan con regímenes de información secreta, reservada o confidencial. Esto genera que una manifestación del poder público altamente intrusiva de los derechos fundamentales opere sin reglas claras, sin trazabilidad suficiente y sin controles verificables *ex ante y ex post*.

1.1. Mecanismos generales de vigilancia estatal

La vigilancia estatal no se materializa a través de una única técnica, sino mediante un conjunto heterogéneo de mecanismos que varían según su objeto, intensidad intrusiva y forma de afectación de derechos. En esta línea, AlSur propone una distinción útil: las técnicas enfocadas en comunicaciones privadas constituyen apenas una tipología dentro de una categoría más amplia de modalidades de vigilancia estatal. Así, junto con la interceptación de comunicaciones y la solicitud de datos o metadatos a empresas de telecomunicaciones, existen otras técnicas, como el uso de (o software espía), el ciberpatrullaje, las tecnologías que interceptan señales de infraestructura móvil, los sistemas de reconocimiento facial y los sistemas de lectura de matrículas vehiculares[8].

a. Intervención de comunicaciones

La intervención de comunicaciones comprende el acceso, escucha, interceptación o registro del contenido de comunicaciones privadas, así como de sus metadatos, tales como tiempo, lugar, duración, emisor, receptor o patrones de contacto[9]. Esta forma de vigilancia resulta especialmente sensible porque compromete la inviolabilidad de las comunicaciones y puede revelar tanto el contenido expresivo de una persona como sus redes con las que interactúa a nivel social, político, profesional o familiar. En buena cuenta, la intervención de comunicaciones no solo permite conocer el contenido comunicacional mismo; sino también permite reconstruir relaciones, rutinas, jerarquías, redes profesionales, vínculos políticos, patrones de conducta, entre otros.

---

8 AlSur, *Tendencias y prácticas de vigilancia en América Latina* (2024).

9 León Pacheco, Lucía. Loc. Cit.

b. Geolocalización

La geolocalización consiste en la identificación de la ubicación geográfica de un dispositivo o persona, ya sea en tiempo real o a partir de registros históricos. Su relevancia jurídica radica en que la localización no solo revela un punto en el espacio, sino patrones de desplazamiento, rutinas, vínculos, lugares de trabajo, asistencia a reuniones, prácticas religiosas, participación política o visitas a determinados espacios sensibles.

Es importante mencionar que los datos de ubicación ofrecen una imagen detallada de la vida cotidiana de una persona y pueden revelar dónde trabaja, vive, se relaciona, practica su culto o busca servicios de salud[10]. La geolocalización, en esta línea, no puede ser entendida como una técnica menor o meramente auxiliar de vigilancia porque esta puede convertirse en una forma indirecta de conocimiento íntimo. Así, geolocalizar no implica únicamente ubicar; más aún puede significar, a través de datos inferidos, el conocer vínculos, hábitos e información sensible.

c. Monitoreo de redes sociales o ciberpatrullaje

El monitoreo de redes sociales, también denominado ciberpatrullaje, se refiere a la vigilancia sistemática de interacciones, publicaciones, perfiles y contenidos en plataformas digitales, con el objetivo de rastrear tendencias, identificar objetivos, anticipar conductas o recolectar información de inteligencia. Esta es una práctica cada vez más utilizada por gobiernos de las Américas, mediante perfilamientos en línea y herramientas de inteligencia de fuentes abiertas[11], lo cual puede colocar a las personas en un estado de sospecha continua por su mera interacción en Internet.

Para nosotros, este mecanismo plantea una tensión particular: aunque muchas de estas fuentes puedan ser públicamente accesibles, su recolección sistemática, automatizada o no, dirigida por parte del Esta-

[10] Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, Loc. Cit.

[11] Ídibem.

do, puede producir efectos de vigilancia intensificada e intromisiones desproporcionadas en los derechos de las personas. En efecto, la publicidad técnica de un dato no elimina necesariamente la expectativa razonable de no ser perfilado, clasificado o monitoreado por el aparato estatal. En buena cuenta, que una información sea públicamente accesible no significa que el Estado pueda convertirla, sin límites, en inteligencia sobre la ciudadanía.

d. Videovigilancia

La videovigilancia comprende el uso de cámaras de circuito cerrado, sistemas de monitoreo urbano u otros dispositivos audiovisuales para registrar de manera continua espacios determinados. Esta forma de vigilancia puede operar en tiempo real o en diferido, y su despliegue exige decisiones sobre la distribución y colocación estratégica de cámaras. Es desde este punto donde se deriva su intensidad intrusiva: esta varía según la ubicación de las cámaras, la finalidad declarada, el tiempo de conservación de imágenes, la existencia de analítica automatizada y la posibilidad de integración con otras bases de datos.

De esta manera, una cámara de seguridad puede operar como una herramienta acotada de prevención situacional o, por el contrario, cuando se integra con analítica de vídeo, reconocimiento facial, bases de datos policiales o sistemas de alerta, se convierte en una infraestructura más amplia de seguimiento, identificación y control social. Así, de acuerdo al tipo de funcionalidades, cantidad, ubicación, interconectividad, un sistema de cámaras de vigilancia se puede convertir en una red de vigilancia urbana masiva.

e. Reconocimiento y/o identificación biométrica

El reconocimiento biométrico comprende tecnologías orientadas a analizar rasgos únicos o relativamente estables de las personas, como rostro, huellas dactilares, voz, iris u otros identificadores corporales, con la finalidad de verificar o identificar individuos de manera remota o automatizada[12]. Esta categoría resulta especialmente relevante porque transforma características corporales en credenciales técnicas de identificación.

[12] León Pacheco, Lucía. Loc. Cit.

La RELE también incluye el reconocimiento facial y la biometría dentro de las tecnologías de vigilancia documentadas en la región, y advierte que su uso indiscriminado en espacios públicos puede constituir una forma de vigilancia masiva, generando dudas sobre necesidad, proporcionalidad, ausencia de evaluaciones de impacto y riesgo de falsos positivos[13]. En definitiva, estamos ante una tecnología que, al usar características corporales de difícil variación, implica una intromisión alta en los derechos de las personas y, por tanto, los estándares de control (por no hablar de prohibición) deberían ser más altos.

1.2. El spyware como forma particularmente intrusiva de vigilancia digital

¿Dónde se ubica el spyware dentro de este mapa general de vigilancia? Entendemos que el software de espionaje representa una de las formas más sofisticadas e intrusivas de vigilancia digital contemporánea pues, al usar todas sus potencialidades de manera conjunta, puede implicar ser a) un medio de intervención de comunicaciones, b) de rastreo y geolocalización, c) de monitoreo de redes y comportamiento digital, d) de videovigilancia y; e) de reconocimiento biométrico: todas al mismo tiempo, de manera remota y sin conocimiento de la persona afectada.

Siguiendo la definición hecha por León[14], entendemos al spyware como "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 diseñado para "acceder a mensajes, llamadas, correos electrónicos, archivos, historial de navegación, ubicación e incluso activar el micrófono o la cámara del dispositivo comprometido". Todo ello, con la capacidad de operar sin dejar rastros visibles, siendo prácticamente indetectable para el usuario común.

[13] Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, Loc. Cit.

[14] León Pacheco, Lucía. Loc. Cit., p. 10.

El informe del Consejo de Europa[15] sobre Pegasus (uno de los spyware más conocidos) refuerza esta caracterización técnica: estamos frente a un software que puede instalarse de manera sigilosa en un smartphone, acceder a todo su contenido, activar cámara y micrófono, y convertir el dispositivo en una herramienta de vigilancia. Además, esta infección se puede realizar mediante ataques de cero clics, inyecciones de red o instalación manual, buscando obtener control del sistema operativo del dispositivo.

Ahora bien, para efectos de este informe, consideramos necesario formular una definición jurídica de spyware, que no dependa únicamente de la etiqueta técnica de "malware", sino de sus capacidades materiales de intrusión. De acuerdo a ello, entenderemos por spyware a toda herramienta de vigilancia digital intrusiva que permite a un operador acceder, monitorear, extraer, copiar, modificar o transmitir información contenida o generada por un dispositivo electrónico, de manera remota o encubierta, sin conocimiento o control efectivo de la persona afectada, con muy difícil capacidad de detección. La información a la que puede acceder son, entre otros, mensajes, llamadas, archivos, contactos, historial de navegación, ubicación, credenciales, comunicaciones cifradas y, eventualmente, la activación de sensores como micrófono o cámara.

Esta definición resulta necesaria porque, desde el punto de vista jurídico, el problema no se agota en si el software fue diseñado como "malicioso" o es presentado comercialmente como una herramienta legítima de investigación criminal, de inteligencia, *lawful interception* o de seguridad nacional: si sus capacidades materiales permiten acceso remoto, encubierto y amplio a un dispositivo personal, corresponde analizarla bajo la definición de spyware. En efecto, cuando una tecnología permite tomar control encubierto de un dispositivo, acceder a información íntima y operar sin señales visibles para la persona afectada, nos encontramos ante una forma de vigilancia de máxima intensidad.

---

[15] Kaldani, Tamar, y Zeev Prokopets. *Pegasus spyware and its impacts on human rights.* Estrasburgo: Council of Europe, 2022. https://rm.coe.int/pegasus-spyware-report-en/1680a6f5d8

Asimismo, a diferencia de mecanismos tradicionales de vigilancia, el software de espionaje puede operar sobre el dispositivo como centro de la vida digital de una persona. El teléfono móvil o la computadora personal, de esta forma, no son simples canales de comunicación, sino repositorios de identidad, memoria, relaciones sociales, desplazamientos, actividad financiera, vida familiar, actividad profesional y participación política[16]. En buena cuenta, intervenir un dispositivo mediante spyware puede equivaler, en términos materiales, a intervenir simultáneamente múltiples dimensiones de la vida privada.

Finalmente, es importante mencionar que el spyware plantea un desafío agravado de rendición de cuentas. Como advierten Anstis y Sprenger, la búsqueda de remedios frente al spyware presenta obstáculos significativos para las personas afectadas, precisamente por la opacidad técnica, las dificultades probatorias, la transnacionalidad de los proveedores y las barreras para acceder a información sobre su adquisición o uso[17]. En la medida que son tecnologías que suelen ser usadas bajo el paraguas de "seguridad nacional", "lucha contra el crimen", "inteligencia" u "orden público", puede existir una gran opacidad respecto de cómo se negocian y se implementan en los Estados que suelen adquirirla.

De la misma forma, ya que el desarrollo de software de espionaje implica, en su mayoría de las veces, la explotación de vulnerabilidades de sistemas operativos avanzados o en constante actualización, su desarrollo suele estar en países con altos niveles de inversión, investigación y desarrollo de *offensive software o security*. En este sentido, países del Sur Global, que dependen de la importación de tecnología (como es el caso del Perú), también se envuelven en la problemática de depender, negociar o contratar con proveedores extranjeros con poco o nulo margen de acción. Además, paradójicamente, son estos países (los que importan esta tecnología) quienes más deterioro democrático tienen, más tendencia hacia al autoritarismo y, por tanto, más posibilidades de uso ilegal, abusivo o represivo de esta tecnología altamente intrusiva.

---

16 En esta línea, visitar https://hiperderecho.org/tdt/ para explorar qué significan las cuentas digitales y las tecnologías en general para las colectivas y diversidades.

17 Anstis, Siena, y Jillian Sprenger. "Civil society and access to justice: challenges of seeking remedy in the global fight against spyware." The International Journal of Human Rights 30, n.º 5 (2026). https://doi.org/10.1080/13642987.2025.2603540

En buena cuenta, de lo expuesto hasta aquí, podemos ver que el spyware debe ser analizado, como veremos más adelante, como una tecnología que conecta tres problemas jurídicos simultáneos: (i) la afectación intensa de derechos fundamentales; (ii) la opacidad de las compras estatales justificadas en seguridad, inteligencia u orden interno; y (iii) la debilidad de los mecanismos de control y rendición de cuentas frente a tecnologías diseñadas precisamente para no ser vistas.

El spyware no afecta un único derecho fundamental ni se agota en la vulneración de la privacidad. Por el contrario, su despliegue compromete un haz complejo de derechos fundamentales y/o garantías constitucionales, algunas afectadas de manera directa por la intrusión técnica en el dispositivo, y otras afectadas de manera indirecta por la potencialidad de la información a recoger y/o el efecto inhibitorio que genera la posibilidad, sospecha o constatación de vigilancia.

DERECHOS FUNDAMENTALES EN TENSIÓN: IMPACTOS DIRECTOS E INDIRECTOS DEL SPYWARE

¿Cuál es, entonces, la diferencia entre afectación directa e indirecta? Por un lado, planteamos que los derechos directamente afectados son aquellos lesionados desde el momento mismo en que el software se infiltra en un dispositivo, accede a información, intercepta comunicaciones o permite control remoto. En cambio, los derechos indirectamente afectados son aquellos cuyo ejercicio se restringe por la potencialidad de la información a ser recogida y el temor razonable a ser observado, identificado, perfilado, expuesto o sancionado. En buena cuenta, el spyware vulnera derechos tanto por su sola instalación en el dispositivo, por lo que extrae (o puede extraer) y por lo que inhibe.

1. DERECHOS AFECTADOS DE FORMA DIRECTA

1.1. Derecho a la vida privada e intimidad

Algunos de los derechos directamente comprometidos son el derecho a la vida privada y el derecho a la intimidad[18]. El Tribunal

[18] STC Exp. N.° 06712-2005-PHC/TC, caso Magaly Medina, ff.jj. 38 a 40

Constitucional ha distinguido entre vida privada e intimidad: la vida privada opera como una categoría más amplia, mientras que la intimidad constituye su núcleo más sensible. Así, la vida privada comprende facetas de la personalidad, relaciones, hábitos y datos que una persona puede legítimamente mantener fuera del conocimiento de terceros; la intimidad, en cambio, refiere al reducto más profundo de la vida personal y familiar.

En esta línea Escartin Cruz[19] sostiene que el uso de spyware constituye una intromisión en la esfera privada en la medida que este permite obtener acceso remoto y encubierto a dispositivos electrónicos, recopilar información privada y acceder a mensajes, llamadas, correos, ubicación, micrófonos o cámaras. En esta línea, podemos afirmar que el spyware no ingresa a un "dato" aislado, sino al espacio digital donde hoy se desarrolla parte sustancial de la vida privada.

Así, cuando un software de espionaje es instalado en un dispositivo cualquiera, al comenzar a recolectar información vinculada a los gustos, interacciones, redes de contacto, mensajes, comentarios, etcétera, se afecta directamente la vida privada (ya que este acceso se da sin consentimiento de la persona afectada). Y, cuando se recopila información relacionada al ámbito personalísimo -información de salud, orientación sexual, confesión religiosa, entre otros vinculados a los datos sensibles-, estamos frente a una vulneración de la intimidad.

1.2. Derecho a la protección de datos personales y/o autodeterminación informativa

El segundo derecho directamente afectado es la autodeterminación informativa (o protección de datos personales), reconocida a partir del artículo 2, inciso 6, de la Constitución, que protege a las personas frente al suministro de informaciones que afecten su intimidad personal y

[19] Escartin Cruz, Shiomara. "Spyware y Debido Proceso en el Sistema Penal Acusatorio: Revisión Crítica del Marco Normativo Mexicano y los Precedentes de la Suprema Corte y la Corte Interamericana." *Ciencia Latina Revista Científica Multidisciplinar* 10, n.º 2 (2026): 4074–4108. https://doi.org/10.37811/cl_rcm.v10i2.23455

familiar por parte de servicios informáticos. El Tribunal Constitucional[20] sostiene que este derecho permite a la persona conocer, actualizar y rectificar informaciones recogidas en bancos de datos. Asimismo, precisó[21] que este derecho consiste en la serie de facultades que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros públicos, privados o informáticos.

De acuerdo a ello, entendemos que el spyware vulnera la autodeterminación informativa porque elimina el control de la persona sobre su información en tres dimensiones esenciales: (i) qué datos se recolectan; (ii) quién accede a ellos; y (iii) para qué finalidad serán tratados. A diferencia de otras formas de tratamiento de datos, el spyware opera sin información previa, sin consentimiento, sin trazabilidad visible y, en consecuencia, sin posibilidad material de ejercer derechos de acceso, rectificación, cancelación u oposición.

En efecto, en la medida que dicha tecnología de vigilancia permite recolectar y almacenar masivamente información sobre los titulares o usuarios de los dispositivos (y, potencialmente, sobre las personas con las que interactúa), incluyendo metadatos y datos de localización[22], se otorga al Estado un alto poder invasivo sobre las personas y, como contraparte, se elimina la capacidad de decisión de la persona sobre su información. En efecto, en estos casos, las personas afectadas por vigilancia digital muchas veces no tienen forma de saber qué información fue sustraída, cuándo ocurrió ni cómo será utilizada en su contra[23].

El derecho a la protección de datos personales (o la autodeterminación informativa) protege el control sobre nuestra información. El spyware lo vulnera sistemáticamente ya que despoja a la persona de toda capacidad de decidir sobre el destino de su información.

---

20 STC Exp. N.° 01797-2002-HD/TC, caso Julia Arellano Serpa, f.j. 8.

21 STC EXP. N. 0 4739-2007-PHD/TC, caso Pesquera Virgen del Valle SAC, f.j. 2.

22 AlSur. Loc. Cit.

23 Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, Loc. Cit.

1.3. Derecho al secreto e inviolabilidad de las comunicaciones

Un tercer derecho directamente afectado es el secreto e inviolabilidad de las comunicaciones y documentos privados, reconocido en el artículo 2, inciso 10, de la Constitución. Esta disposición normativa establece que las comunicaciones, telecomunicaciones y sus instrumentos solo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez, con las garantías previstas en la ley. El Tribunal Constitucional[24] ha señalado que este derecho tiene eficacia sobre todas las personas, entidad privadas y estatales, pues garantiza la no penetración de las comunicaciones por terceros, sean estos órganos públicos o particulares. Asimismo, ha precisado que el derecho se vulnera cuando se produce una interceptación de comunicaciones o cuando se accede al conocimiento de lo comunicado sin autorización[25].

De acuerdo a ello, el spyware afecta este derecho porque permite acceder a comunicaciones protegidas, incluso cuando estas se encuentran cifradas o alojadas dentro de aplicaciones de mensajería, existiendo la potencialidad de acceder a aquellas que no han sido objeto de autorización judicial, de existir. El informe del Consejo de Europa[26] sobre Pegasus explica que, una vez instalado, Pegasus puede recolectar datos del dispositivo y transmitirlos al atacante, incluyendo llamadas, mensajes, correos, ubicación, fotografías, videos, historial de navegación y datos de aplicaciones como WhatsApp, Telegram, Skype, Gmail o iMessage.

No obstante ello, el problema constitucional no se limita a la interceptación clásica de una llamada o correo. En el caso del spyware, el acceso se produce desde el dispositivo mismo, lo que permite capturar comunicaciones antes, durante o después de su transmisión. En buena cuenta, el software espía desplaza el problema desde la "interceptación de comunicaciones" hacia la "intervención del entorno comunicacional completo" de la persona.

---

24 STC Exp. N.° 2863-2002-AA/TC

25 STC Exp. N.° 2863-2002-AA/TC

26 Kaldani, Tamar, y Zeev Prokopets. Loc. Cit.

Como explicamos previamente, el spyware, para que tenga efectividad, suele instalarse en el dispositivo sin el conocimiento y/o consentimiento del usuario. Respecto de este supuesto, estaríamos frente al problema clásico de interceptación de comunicaciones. No obstante, incluso en el supuesto de existir orden judicial que habilite su uso, cabe responder la pregunta sobre si su aplicación resulta proporcional respecto de los derechos fundamentales afectados.

1.4. Derecho al debido proceso, derecho de defensa y licitud probatoria

El cuarto derecho directamente afectado es el debido proceso y, de manera específica, el derecho de defensa. El artículo 139, inciso 3, de la Constitución reconoce la observancia del debido proceso y la tutela jurisdiccional y, en esta línea, el Tribunal Constitucional ha señalado que el debido proceso garantiza el respeto de los derechos y garantías mínimas que debe tener todo justiciable para que una causa pueda tramitarse y resolverse con justicia[27]. En cuanto al derecho de defensa, como contenido del debido proceso, el TC[28] sostuvo que este derecho impide que los justiciables queden en estado de indefensión y, en el proceso penal, garantiza que el imputado ejerza su defensa desde que toma conocimiento de la atribución de un hecho delictivo, así como el derecho a contar con defensa técnica.

De acuerdo a ello, el uso de software de espionaje afecta el debido proceso cuando la persona vigilada, no sabe que está siendo investigada, no puede cuestionar la legalidad de la medida, no puede controlar la cadena de custodia de la información obtenida y no puede discutir oportunamente la licitud de la prueba. En efecto, Escartin Cruz[29] advierte que la naturaleza encubierta del spyware dificulta la supervisión judicial efectiva y puede generar riesgos significativos para el respeto de las garantías procesales.

---

27 STC Exp. N.° 02322-2021-PA/TC

28 STC Exp. N.° 00808-2022-PHC/TC.

29 Escartin Cruz, Shiomara. Loc. Cit.

En buena cuenta, cuando el spyware se utiliza sin habilitación legal clara, sin autorización judicial suficiente (con la dudosa proporcionalidad en su uso como mencionamos previamente) o fuera del marco de una investigación legítima contamina el proceso penal desde su fuente probatoria.

1.5. Dignidad humana, autonomía personal y libre desarrollo

Finalmente, un derecho fundamental directamente comprometido es la dignidad humana y su relación con el libre desarrollo de la personalidad. El artículo 1 de la Constitución establece que la defensa de la persona humana y el respeto de su dignidad son el fin supremo de la sociedad y del Estado; el artículo 2, inciso 1, reconoce el derecho al libre desarrollo y bienestar. El Tribunal Constitucional ha sostenido que la dignidad de la persona humana constituye un valor y principio constitucional que impide tratar a una persona como un simple medio[30]. Asimismo, en materia de libre desarrollo, ha recordado que, dado que la defensa de la persona humana y el respeto de su dignidad son el fin supremo de la sociedad y del Estado, no cabe tratar a un ser humano de manera incompatible con su autonomía, libertad e independencia[31].

De acuerdo a ello, entendemos que el spyware afecta la dignidad humana porque transforma a la persona en objeto permanente de observación, extracción y análisis, vaciándola de toda cualidad y/o valor subjetivo. La persona deja de ser sujeto de derechos para convertirse en una fuente de datos explotable por el aparato estatal o por terceros que operan en su nombre bajo supuestos de "seguridad nacional" o cualquiera de sus variantes.

Un nivel de afectación tan grave a los derechos fundamentales, donde la cantidad de información extraída penetra de forma tan grave en la personalidad, la autonomía, la privacidad e intimidad, no puede ser entendida únicamente como una mera tecnología. Esta es, en efecto, una tecnología de vigilancia que vacía de humanidad a la persona que es

30 STC Exp. N.° 02101-2011-PA/TC.

31 STC Exp. N.° 01146-2021-AA/TC

objeto de ella, al considerarla como objeto de extracción informativa, y, por tanto, afecta su dignidad.

2. DERECHOS AFECTADOS DE FORMA INDIRECTA: EL EFECTO INHIBITORIO

Ahora bien, es importante mencionar que existen una serie de derechos que se ven afectados, de manera indirecta, cuando el Estado decide usar esta tecnología. Es decir, derechos que no se ven afectados en un primer momento pero que, dependiendo de diferentes variables contextuales, pueden verse vulnerados. A continuación los desarrollaremos.

2.1. Libertad de expresión, opinión e información

El primer derecho indirectamente afectado es la libertad de expresión, opinión e información, reconocida en el artículo 2, inciso 4, de la Constitución. Esta disposición protege las así llamadas libertades informativas que deben ejercerse sin previa autorización, censura ni impedimento. El Tribunal Constitucional, en la STC Exp. N.° 00905-2001-AA/TC, distinguió entre libertad de expresión y libertad de información. La primera garantiza la transmisión de ideas, pensamientos, juicios de valor u opiniones; la segunda protege la búsqueda, recepción y difusión de información veraz de relevancia pública.

Respecto a ello, el spyware afecta indirectamente la libertad de expresión porque produce un efecto inhibitorio o chilling effect. La persona que sospecha que puede ser vigilada restringe sus opiniones, evita investigar temas sensibles o abandona conversaciones políticas, periodísticas o activistas. En efecto, AlSur[32] y la RELE[33] sostienen que el riesgo de ser objetivo de vigilancia lleva a las personas a autocensurarse, alterando y limitando la forma en que se expresan y comunican con otras

[32] AlSur. Loc. Cit.

[33] Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, Loc. Cit.

personas. De hecho, la mera posibilidad de estar bajo vigilancia puede conducir a comportamientos de autocensura[34].Y, de hecho, quienes sospechan ser objeto de vigilancia, son personas clave en la difusión información y referentes de opinión pública, como periodistas que investigan regímenes autoritarios, lideresas medioambientales, dirigentes políticas, entre otros casos. Por ello, la censura individual y selectiva de personajes clave para la democracia, tiene además de una afectación directa personal, una afectación indirecta en el derecho a la libertad de expresión e información de la sociedad.

2.2. Secreto profesional y protección de fuentes periodísticas

El secreto profesional y, dentro de ello, la protección de fuentes periodísticas, se encuentra en el artículo 2, inciso 18, de la Constitución. Este se constituye como una garantía-derecho que "supone una obligación para el profesional (abogado, notario, médico, periodista, etc.) de mantener en reserva o confidencialidad las confesiones, hechos, situaciones o cualquier noticia de la que haya tomado conocimiento, o que se le haya confiado de modo directo en su condición de profesional o técnico en determinada arte o ciencia"[35]. De esta forma, el Tribunal Constitucional también manifiesta que esta garantía "resulta fundamental cuando la profesión u oficio guarda estrecha relación con el ejercicio de otras libertades públicas, como es el caso de los periodistas respecto de la libertad de información y expresión, o de los abogados con relación al ejercicio del derecho de defensa".

De acuerdo a ello, el software espía afecta indirectamente este derecho-garantía porque compromete la relación entre periodistas y fuentes (o abogados y clientes). Si un teléfono puede ser intervenido de manera remota y encubierta, las fuentes dejan de tener garantías razonables de confidencialidad, y el periodismo de investigación pierde condiciones materiales de funcionamiento. De la misma forma, si un abogado o médico puede ver intervenido su teléfono en cualquier momento, el secreto profesional respecto del cliente o paciente es impo-

[34] Anstis, Siena, y Jillian Sprenger. Loc. Cit.

[35] STC Exp. N.O 7811-2005-PA/TC

sible de garantizar. Así, este secreto se rompería cuando se interviene el dispositivo o cuando la persona deja de confiar en el profesional si sabe o intuye que sus comunicaciones podrían no estar resguardadas constitucionalmente.

En buena cuenta, vigilar a un periodista, un abogado o un médico no afecta solo a ese periodista: afecta a sus fuentes, clientes y pacientes. No hay garantías de un normal desenvolvimiento profesional en un entorno ampliamente vigilado.

2.3. Libertad de reunión y derecho de asociación

El tercer grupo de derechos indirectamente afectados comprende la libertad de reunión y el derecho de asociación. El artículo 2, inciso 12, de la Constitución reconoce el derecho de reunión pacífica y sin armas; el artículo 2, inciso 13, reconoce el derecho a asociarse y constituir diversas formas de organización jurídica sin autorización previa. De un lado, el derecho de asociación permite integrarse con otras personas de manera libre y permanente en función de determinados objetivos lícitos; mientras que el derecho de reunión, aunque igualmente relevante, tiene un carácter episódico o circunstancial[36].

En este contexto, el spyware afecta estos derechos porque podría generar que las personas eviten asistir a protestas, reuniones, colectivos, sindicatos, partidos o espacios de defensa de derechos por temor a ser identificadas como "blancos" de inteligencia. Anstis y Sprenger[37] advierten que el spyware puede afectar la libertad de reunión pacífica, pues las tecnologías digitales son esenciales tanto para organizar asambleas presenciales como para sostener asambleas digitales.

En consecuencia, la vigilancia de comunicaciones produce efectos en la protesta, asociación y participación pública, precisamente porque la expectativa de vigilancia altera la forma en que las personas se organizan y comunican[38]. Cuando se usa spyware el Estado puede conocer

[36] STC Exp. N.° 08766-2006-PA/TC

[37] Anstis, Siena, y Jillian Sprenger. Loc. Cit.

[38] AlSur. Loc. Cit.

quién se reúne con quién antes de que la reunión ocurra: la libertad de reunión, de esta forma, pierde espontaneidad, confianza y capacidad organizativa.

2.4. Derecho a la integridad física, psíquica y moral

Un cuarto derecho afectado, aunque muchas veces por conexión o consecuencia, es el derecho a la integridad física, psíquica y moral, reconocido en el artículo 2, inciso 1, de la Constitución. El Tribunal Constitucional[39] ha señalado que el derecho a la integridad personal protege la incolumidad de la persona humana en sus dimensiones moral, psíquica y física. Respecto de la integridad física, precisa que protege frente a intervenciones en el cuerpo sin consentimiento; y, por extensión, la integridad psíquica y moral protege frente a afectaciones a la estabilidad emocional de la persona[40].

En esta línea, el spyware puede afectar la integridad psíquica y moral cuando produce ansiedad, miedo, aislamiento, sensación de vulnerabilidad permanente o autocensura derivada de la vigilancia (cuando la persona tiene conocimiento o sospechas razonables de que está siendo vigilada). Anstis y Sprenger[41] documentan que el software de espionaje contra sociedad civil, especialmente periodistas y defensores, amenaza la dignidad, seguridad y protección digital de las víctimas, y puede generar riesgos físicos cuando permite acceso en tiempo real a ubicación y comunicaciones.

Por su lado, la RELE también ha señalado que la vigilancia digital, en algunos casos, ha precedido a daños físicos y forma parte de procesos continuos de represión y persecución[42]. En este punto, podemos afirmar que el spyware no es una afectación "solo digital" o de datos o de derechos abstractos: cuando permite ubicar, exponer, intimidar o per-

39 STC Exp. N.° 05312-2011-PA/TC.

40 STC Exp. N.° 05312-2011-PA/TC.

41 Anstis, Siena, y Jillian Sprenger. Loc. Cit.

42 Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, Loc. Cit.

seguir a una persona, la frontera entre daño informacional y daño físico o psicológico se desdibuja y se ven mezclados entre sí.

2.5. Libertad de pensamiento, conciencia y religión

La libertad de conciencia y religión se encuentra reconocida en el artículo 2, inciso 3, de la Constitución. A ello se suma el artículo 2, inciso 18, que protege la reserva sobre convicciones políticas, filosóficas, religiosas o de cualquier otra índole. El efecto del software de espionaje sobre este derecho es principalmente indirecto, aunque no por ello menor. En efecto, si una persona sabe o sospecha que su dispositivo puede ser intervenido, puede restringir búsquedas, lecturas, conversaciones espirituales, consultas íntimas o intercambios vinculados a sus convicciones.

No obstante ello, es importante matizar lo enunciado. No toda vigilancia digital afecta automáticamente el fuero interno de la persona, pues los pensamientos no exteriorizados permanecen fuera del alcance técnico directo del Estado. Sin embargo, cuando la exploración de ideas, creencias o convicciones se realiza mediante búsquedas, mensajes, notas, lecturas o conversaciones digitales, el spyware puede convertir ese proceso interno de formación de conciencia en información susceptible de captura.

Más aún, teniendo en cuenta que, hoy en día, hay quienes conciben la interacción con sus dispositivos como un ámbito a través del cual se materializa o forma la convicción interna, el riesgo de afectación crece aún más. Si bien el spyware no lee la mente, sí puede vigilar los rastros digitales mediante los cuales una persona forma, explora o expresa sus convicciones.

En conclusión, el spyware debe ser analizado como una tecnología de afectación constitucional múltiple. Directamente, compromete la vida privada, la intimidad, la autodeterminación informativa, el secreto de comunicaciones, el debido proceso, la dignidad y la integridad. Indirectamente, inhibe la libertad de expresión, la prensa, la reunión, la asociación, la libertad de pensamiento, conciencia y religión

En buena cuenta, el software espía no es únicamente una herramienta de investigación o inteligencia, sino una tecnología capaz de alterar las condiciones materiales de ejercicio de derechos en una sociedad democrática. Por ello, al ser una tecnología altamente intrusiva y lesiva, resulta necesario analizar cómo los diferentes marcos normativos que podrían regular su adquisición y uso dialogan entre sí, qué aspectos generan opacidad y qué vacíos o lagunas normativas nos pueden generar alarma en torno a ello.

MARCO LEGAL DE LAS CONTRATACIONES DEL ESTADO PARA TECNOLOGÍAS DE VIGILANCIA (Y SPYWARE)

1. RÉGIMEN GENERAL DE CONTRATACIONES (LEY 32069)

En este punto, corresponde partir de una premisa metodológica central: el régimen de contrataciones públicas no puede ser entendido únicamente como un conjunto de reglas procedimentales orientadas a seleccionar proveedores, adjudicar contratos o ejecutar prestaciones. En realidad, bajo la Ley N.° 32069, Ley General de Contrataciones Públicas (en adelante, la Ley de Contrataciones), el sistema de contratación estatal se estructura a partir de principios jurídicos que cumplen una función rectora, interpretativa y finalista sobre todo el ciclo de compra pública.

Esta precisión resulta particularmente importante cuando analizamos la eventual adquisición estatal de tecnologías de vigilancia, como el spyware. En este tipo de bienes o servicios, la contratación no solo compromete eficiencia presupuestal o idoneidad técnica, sino también derechos fundamentales, control público y límites al poder estatal. Así, los principios operan como el primer filtro jurídico frente a adquisiciones que, por su naturaleza intrusiva, no pueden ser eva-

luadas únicamente bajo criterios de oportunidad administrativa o conveniencia operativa.

1.1. Rol de los principios en el marco legal de contrataciones del estado

Los principios en la Ley de Contrataciones del Estado cumplen un rol fundamental como ejes rectores, parámetros de actuación y herramientas de interpretación de todo el sistema de adquisición pública[43][44]. Su función, lejos de ser puramente declarativa, posee una preeminencia valorativa sobre las demás normas, lo que implica que su inobservancia puede ser considerada más grave que el incumplimiento de una regla técnica o procedimental[45].

En este sentido, se puede identificar que los principios

> (...) cumplen una triple función para el mejor desenvolvimiento de las decisiones cotidianas de las diversas fases de la contratación administrativa, desde su planeamiento hasta la liquidación contractual. Cumplen, en primer lugar, un rol de función teleológica general, en la medida que coadyuvan a identificar cuáles son las finalidades que deben atender las normas de contrataciones, de modo que las reglas de selección, ejecución y liquidación, por ejemplo, no pueden entenderse sin comprender cabalmente los principios de la contratación administrativa.
>
> Luego, cumplen una función interpretativa integral del ordenamiento sobre la materia, de manera que una regla de las bases de un proceso de selección no puede interpretarse de modo literal o de manera aislada sino en función precisamente de los principios

[43] Morón Urbina, Juan Carlos, y Zita Aguilera B. *Aspectos jurídicos de la contratación estatal.* Colección Lo Esencial del Derecho 9. Lima: Fondo Editorial de la Pontificia Universidad Católica del Perú, 2019

[44] Moreno Molina, José Antonio. "Principios Generales de la Contratación Pública en el Reciente Derecho Internacional, Europeo y de América Latina". *Derecho & Sociedad*, n.º 44 (2015): 55–65

[45] Morón Urbina, Juan Carlos. "Los principios inspiradores de la contratación administrativa y sus aplicaciones prácticas". *THEMIS: Revista de Derecho,* n.º 52 (2006): 189–210

que le inyectan una personalidad y sentido propio. Finalmente, cada principio cumple una función integradora respecto a los vacíos que pueda presentar el ordenamiento sobre la materia contractual[46].

1.2. Principio de transparencia y principio de publicidad

Dentro del marco de contrataciones estatales, dos principios sirven como parámetro de control para la compra y/o adquisición de spyware: el principio de publicidad y el de transparencia y facilidad de uso.

a) Principio de publicidad: El artículo 5, literal g), de la Ley N.° 32069 establece que las entidades contratantes deben garantizar que el proceso de contratación sea objeto de publicidad y difusión, con la finalidad de promover la libre concurrencia, la competencia efectiva, la supervisión y el control de las contrataciones. En este sentido, la publicidad cumple una función de visibilidad externa del proceso contractual en tanto y en cuanto permite que el mercado, la ciudadanía y los órganos de control puedan conocer que una contratación existe, bajo qué modalidad se realiza y qué decisiones adopta la entidad.

b) Principio de transparencia y facilidad de uso: De otro lado, el artículo 5, literal i), dispone que las actuaciones y decisiones del proceso de contratación deben basarse en reglas y criterios claros y accesibles, garantizando acceso público y oportuno a la información, salvo las excepciones previstas por ley. Asimismo, exige que las plataformas, sistemas y trámites sean sencillos, oportunos, seguros y brinden información confiable, oficial y útil. De acuerdo a ello, la transparencia cumple una función de comprensión y trazabilidad. No basta con que la información sea publicada; debe ser accesible, clara, oportuna y útil para participar, competir, supervisar o controlar el proceso.

[46] Morón Urbina, Juan Carlos, y Zita Aguilera B. Loc. Cit.

La diferencia principal entre ambos principios puede formularse así: la publicidad se orienta a que el proceso de contratación sea conocido y difundido; la transparencia, en cambio, exige que la información disponible sea clara, accesible y funcional para comprender las decisiones adoptadas. Así, la diferencia que encontramos es que el principio de transparencia parece estar orientado al procedimiento de contratación específico, dirigido a los participantes y postores; mientras que la publicidad aplica al total de actuaciones de contrataciones y todos los procesos, dirigido a facilitar la supervisión y control de las contrataciones (por parte de la ciudadanía y otros agentes de control externo[47]).

No obstante esta diferencia, para efectos del presente informe trataremos los principios de publicidad y transparencia de manera conjunta o indistinta, salvo que la distinción sea necesaria. Ello se debe a que, en materia de adquisición de spyware, ambos principios cumplen una misma función democrática: evitar que la contratación pública de tecnologías intrusivas se realice en condiciones de opacidad, reserva injustificada o imposibilidad práctica de control.

2. TIPOS DE PROCEDIMIENTOS DE SELECCIÓN Y MECANISMOS DE CONTROL PARA EL SPYWARE

Existen dos grandes regímenes dentro de la Ley N.° 32069: (i) los procedimientos de selección competitivos y (ii) los procedimientos de selección no competitivos. Esta distinción es central para el análisis de la compra y/o adquisición de software de espionaje porque el nivel de publicidad, concurrencia, trazabilidad y control varía sustancialmente según el régimen empleado.

---

47 Diferencia que se aplica de manera inversa en el régimen español de contrataciones "la publicidad persigue dar a conocer la actividad que lleva a cabo la Administración Pública en un determinado procedimiento de contratación, mientras que la transparencia buscaría permitir a los ciudadanos conocer qué sucede en el seno de las administraciones públicas en relación a la contratación pública". Cerrillo i Martínez, A. (1998): *Publicidad y transparencia en el Parlamento Europeo*. Revista De las Cortes Generales, 45, 7-46.; citado en Miranzo-Díaz, J. "El principio de transparencia en el derecho global de la contratación pública". *Revista de Derecho Administrativo* (18), 276–302. Recuperado a partir de https://revistas.pucp.edu.pe/index.php/derechoadministrativo/article/view/22865

¿Dónde aparece el punto crítico? En que la compra de spyware puede ingresar al sistema de contrataciones públicas por más de una vía. Puede adquirirse mediante un procedimiento competitivo, como bien o servicio tecnológico; puede contratarse directamente bajo la causal de proveedor único o derechos exclusivos; o puede tramitarse bajo la causal más problemática: contrataciones de las Fuerzas Armadas, la PNP o los componentes del Sistema de Inteligencia Nacional (en adelante, SINA) declaradas de carácter secreto, secreto militar o por razones de orden interno.

Como desarrollaremos, no toda compra de spyware es jurídicamente opaca por el solo hecho de ser spyware. La opacidad se intensifica cuando la compra se desplaza hacia un procedimiento no competitivo y, de manera especialmente grave, cuando se invoca la causal de secreto.

2.1. Los dos regímenes de contratación: procedimientos competitivos y no competitivos

La Ley N.° 32069 parte de una regla general: las entidades contratantes realizan procedimientos de selección para contratar los requerimientos previstos en su planificación, tomando en cuenta el objeto, la cuantía y los principios del sistema de contratación pública. En esa línea, el artículo 54.1 identifica como procedimientos competitivos la licitación pública para bienes y obras, y el concurso público para servicios. A su vez, el artículo 54.3 establece que las entidades realizan procedimientos competitivos, salvo las excepciones previstas por la propia ley.

De acuerdo a ello, y conforme a los principios de la propia ley, el procedimiento competitivo es la regla; el procedimiento no competitivo, la excepción. Allí donde hay competencia, publicidad, pluralidad de ofertas y evaluación comparativa, existe una mayor posibilidad de control ex ante y ex post; sin embargo, cuando no hay competencia, en cambio, el control depende de la solidez del expediente, la motivación reforzada y la posibilidad de acceder posteriormente a la información.

En efecto, el artículo 55.1 de la Ley N.° 32069 autoriza la contratación directa "sin perjuicio de la sujeción a los principios que rigen las contrataciones públicas". Esta fórmula es relevante porque impide entender los procedimientos no competitivos como zonas liberadas de los principios de publicidad, transparencia, integridad, valor por dinero y responsabilidad.

Así, los procedimientos no competitivos constituyen un régimen especial que limitan la operatividad de los principios del régimen de contrataciones y, por ello, deben ser interpretados restrictivamente. Si la regla es competir, toda excepción debe estar motivada, documentada y sometida a control. Lo contrario convertiría la contratación directa en una puerta trasera para eludir la transparencia.

2.2. Compra de spyware mediante procedimiento competitivo: publicidad, competencia y trazabilidad relativa

A continuación, corresponde analizar el escenario menos opaco: la adquisición de spyware mediante un procedimiento competitivo. Si una entidad estatal decidiera adquirir una herramienta de vigilancia digital a través de una licitación pública, concurso público u otra modalidad competitiva aplicable, el procedimiento exigiría, por su propia naturaleza, ciertos niveles de publicidad. Estos son:

1. El requerimiento formulado por la entidad, incluyendo la necesidad pública invocada y las características técnicas solicitadas.
2. Las bases del procedimiento, donde deberían aparecer condiciones de admisión, requisitos técnicos, criterios de evaluación, obligaciones contractuales y eventuales exigencias de soporte, mantenimiento o capacitación.
3. La pluralidad de postores, si existiera concurrencia efectiva.
4. Las ofertas técnicas y económicas, al menos en la medida en que no contengan información legítimamente protegida.
5. La adjudicación y el contrato, incluyendo monto, proveedor, objeto y condiciones generales de ejecución.

6. La ejecución contractual, mediante conformidades, pagos, ampliaciones, adendas o controversias.

De esta manera, incluso si el objeto contractual fuese una tecnología intrusiva, existiría un rastro administrativo capaz de ser auditado, fiscalizado y eventualmente solicitado mediante la Ley de Transparencia y Acceso a la Información Pública (o de conocimiento público a través de las plataformas digitales de compras públicas). De la misma forma, se garantiza la competencia que, en teoría, permite evaluar distintos proveedores y poder elegir el que ofrecerá una mejor propuesta en términos de costos y beneficios.

No obstante ello, debemos introducir una matización: que un procedimiento sea competitivo no significa que sea automáticamente legítimo desde una perspectiva de derechos fundamentales. Una compra competitiva de spyware podría seguir siendo problemática si carece de evaluación de impacto, autorización legal suficiente o las salvaguardas mínimas que desarrollaremos en la última parte de este informe.

Sin embargo, desde el punto de vista del control y la rendición de cuentas en la contratación estatal, el procedimiento competitivo sí ofrece una ventaja mínima: permite reconstruir quién compró, qué compró, a quién le compró, por cuánto, bajo qué especificaciones y con qué justificación. De esta forma, el procedimiento competitivo no elimina el riesgo de abuso, pero sí reduce el riesgo de invisibilidad.

2.3. Procedimientos no competitivos: contratación directa y riesgo de opacidad

De otro lado, los procedimientos de selección no competitivos modifican sustancialmente la lógica de contratación. Conforme al Reglamento de la Ley N.° 32069, el proceso se inicia con el requerimiento y mantiene ciertas actuaciones preparatorias, pero excluye la interacción con el mercado. Asimismo, la fase de selección consiste únicamente en la invitación al proveedor identificado y la presentación de sus ofer-

tas técnica y económica. Además, no se designan evaluadores ni existe evaluación técnica o económica de ofertas en sentido comparativo.

Esta estructura revela el núcleo del problema: en un procedimiento no competitivo, la entidad no abre una competencia entre proveedores, sino que identifica a uno y negocia directamente con este. Ello no es necesariamente ilegal, pues la Ley autoriza supuestos específicos. Sin embargo, sí exige un estándar reforzado de justificación, precisamente porque se elimina la disciplina que genera la competencia.

En efecto, el artículo 102.3 del Reglamento exige que la resolución que aprueba el procedimiento no competitivo cuente obligatoriamente con informes técnico y legal sobre la necesidad de la contratación y la procedencia de la causal invocada. Además, el artículo 102.5 establece que la resolución aprobatoria y los informes que la sustentan deben publicarse en la Pladicop (Plataforma Digital para las Contrataciones Públicas) dentro de los diez días hábiles siguientes, salvo el supuesto previsto en el literal m) del artículo 55.1 de la Ley.

De acuerdo con ello, nosotros entendemos que la contratación directa no es, per se, una contratación secreta. Salvo la causal del literal m) -que posteriormente abordaremos-, el régimen conserva mecanismos mínimos de publicidad posterior: resolución, informes técnico y legal, expediente y posibilidad de control vía transparencia. El procedimiento no competitivo reduce la competencia, pero no necesariamente elimina la trazabilidad o la publicidad de la compra. El problema, entonces, como veremos, aparece cuando la contratación directa se cruza con la clasificación por secreto, secreto militar u orden interno.

a) Proveedor único o derechos exclusivos

Una primera vía posible para adquirir spyware mediante contratación directa es el literal d) del artículo 55.1 de la Ley N.° 32069, aplicable cuando los bienes o servicios solo puedan obtenerse de un determinado proveedor o cuando este posea derechos exclusivos respecto de ellos. El Reglamento desarrolla esta causal señalando que debe verifi-

carse que los bienes, servicios o consultorías solo puedan obtenerse de un determinado proveedor en el mercado peruano, debido a patentes vigentes, permisos, exclusividad de distribución u otras fuentes documentadas que acrediten dicha condición.

Esta causal podría ser relevante para el software de espionaje por una razón evidente: al tratarse de software propietario, usualmente protegido por derechos de propiedad intelectual, licencias exclusivas, know-how técnico, infraestructura cerrada, actualizaciones controladas por el proveedor o distribución mediante intermediarios autorizados, la entidad podría alegar que solo un determinado proveedor puede ofrecer la herramienta requerida. En efecto, en ciertos mercados tecnológicos, particularmente de software especializado, puede ocurrir que una solución solo sea ofrecida por un proveedor específico o que un distribuidor cuente con exclusividad acreditada. Sin embargo, la existencia de derechos exclusivos no debe ser utilizada como atajo para evitar preguntas básicas sobre necesidad, proporcionalidad, finalidad pública, riesgos en derechos fundamentales y alternativas menos intrusivas.

En este supuesto, la compra de spyware seguiría siendo controlable en cierto grado. Así, la entidad, por lo menos:

1. Debería sustentar técnicamente por qué requiere esa herramienta y no otra.
2. Debería acreditar documentalmente la exclusividad, patente o fuente equivalente.
3. Debería aprobar la contratación mediante resolución sustentada en informe técnico y legal.
4. La resolución e informes deberían publicarse en la Pladicop, conforme al artículo 102.5 del Reglamento.
5. La información podría ser solicitada mediante acceso a la información pública, sin perjuicio de eventuales reservas parciales legalmente justificadas.

Así, si bien la causal de proveedor único puede ser riesgosa porque elimina competencia, esta no debería eliminar la transparencia y publicidad de la contratación. Si una entidad compra spyware invocando derechos exclusivos del proveedor, el Estado mantiene la carga de explicar por qué esa solución era necesaria, por qué no existían alternativas y bajo qué condiciones contractuales se adquirió.

b) Contrataciones secretas de Fuerzas Armadas, PNP y SINA

El supuesto verdaderamente crítico es el previsto en el artículo 55.1, literal m), de la Ley N.° 32069. Esta causal permite la contratación directa de bienes, servicios u obras realizadas por las Fuerzas Armadas, la Policía Nacional del Perú y los componentes del Sistema de Inteligencia Nacional que hayan sido declaradas de carácter secreto, secreto militar o por razones de orden interno, mediante decreto supremo refrendado por el Ministerio de Economía y Finanzas y el sector correspondiente, con opinión previa favorable de la Contraloría General de la República.

El Reglamento añade una precisión importante: esta causal no aplica a bienes, servicios u obras de carácter administrativo u operativo necesarios para el normal funcionamiento de las Fuerzas Armadas, la PNP o los componentes del SINA. Asimismo, establece que la opinión favorable de la Contraloría se sustenta en comprobar que el objeto de contratación esté incluido en la lista de bienes, servicios y obras declarados de carácter secreto militar o de orden interno.

De acuerdo con ello, utilizar esta causal para la compra de bienes y/o servicios tiene tres requisitos reforzados:

1. Declaración mediante decreto supremo, refrendado por el MEF y el sector correspondiente.
2. Opinión previa favorable de la Contraloría General de la República.
3. Inclusión del objeto contractual en una lista de bienes, servicios u obras declarados secretos, secretos militares o de orden interno.

En apariencia, la norma contiene un mínimo de salvaguardas. Sin embargo, la pregunta realmente importante es otra: ¿estas salvaguardas funcionan realmente como controles materiales o solo como condiciones formales dentro de un circuito opaco? Al respecto, León[48] documentó un problema especialmente grave: cuando se solicitó acceso a la lista y a documentos vinculados a este supuesto de excepción, la Presidencia del Consejo de Ministros respondió que la información requerida no existía, a pesar de que la disposición reglamentaria de declaración mediante decreto supremo existía desde 2018.

Este hallazgo es particularmente relevante porque si la lista no existe, no es pública o no puede ser identificada por la propia entidad llamada a conocerla, el control previo queda severamente debilitado. El uso del paraguas de secreto, en este caso, se presenta como gran puerta a la opacidad del control de la adquisición de tecnologías de la vigilancia.

En este punto, es importante mencionar que la diferencia entre la causal de proveedor único y la causal secreta es decisiva. En el proveedor único, el procedimiento no competitivo conserva trazabilidad pública posterior. En cambio, en la causal del literal m), el propio Reglamento excluye la publicación de la resolución aprobatoria y de los informes que sustentan la contratación. Así, el artículo 102.5 establece la publicación de dichos documentos, salvo en el supuesto previsto en el literal m) del artículo 55.1 de la Ley.

Esto genera un efecto jurídico acumulativo, a saber:

1. No hay competencia abierta.
2. No hay interacción con el mercado.
3. No hay evaluación comparativa de ofertas.
4. Se invita únicamente al proveedor identificado.
5. La contratación se justifica por secreto, secreto militar u orden interno.

[48] León Pacheco, Lucía. Loc. Cit.

6. La resolución e informes sustentatorios no se publican.
7. El acceso posterior por transparencia puede ser denegado bajo causales de información secreta o reservada.
8. La fiscalización ciudadana se vuelve prácticamente inviable.

De esta manera, el literal m) no solo elimina la competencia, sino que también debilita la publicidad posterior. La consecuencia es que, tratándose de spyware, esta causal puede convertirse en el mecanismo más opaco de adquisición pública.

No obstante ello, debemos precisar que el secreto puede tener una función legítima en ciertos ámbitos de defensa, inteligencia u orden interno. Nosotros no sostenemos que toda reserva sea inválida per se. Sin embargo, cuando el objeto contractual es una tecnología capaz de intervenir comunicaciones, extraer datos de dispositivos, acceder a información íntima y afectar libertades públicas, el secreto no debería operar, bajo ningún supuesto, como la regla general de gestión de compras administrativas.

3. RECAPITULACIÓN: FORMAS DE ADQUISICIÓN DE SPYWARE POR EL ESTADO

De acuerdo a lo hasta aquí expuesto, la adquisición de spyware podría transitar por tres rutas jurídicamente diferenciables:

a) Ruta competitiva: La compra se realiza mediante licitación, concurso u otra modalidad competitiva. Es peligrosa desde la perspectiva de derechos si carece de salvaguardas, pero es rastreable en términos contractuales.

b) Ruta no competitiva por proveedor único o derechos exclusivos: La compra se realiza directamente porque el software, licencia, patente o distribución solo puede obtenerse de un proveedor determinado. Reduce competencia, pero conserva cier-

tos mecanismos de publicidad posterior, publicación de informes, expediente y control vía acceso a información pública.

c) Ruta no competitiva secreta: La compra se realiza por Fuerzas Armadas, PNP o SINA bajo carácter secreto, secreto militar u orden interno. Aquí se acumulan la ausencia de competencia, la ausencia de publicación de informes, la reserva del objeto contractual y la posible denegatoria posterior de acceso a información pública.

Nosotros consideramos que esta tercera ruta es la más problemática para una tecnología como el spyware. En efecto, si el spyware se compra mediante procedimiento competitivo, hay riesgos de derechos, pero existe una mínima trazabilidad pública. Si se compra por proveedor único, hay riesgos de concentración y discrecionalidad, pero subsisten mecanismos de control documental. Si se compra bajo la causal secreta del literal m), el riesgo se agrava cualitativamente: la herramienta más intrusiva se adquiere mediante el mecanismo menos visible.

Por ello, el punto más sensible no está únicamente en que el Estado pueda comprar spyware (que sí es un problema en sí mismo), sino en que pueda hacerlo mediante un procedimiento no competitivo, sin concurso público, con proveedor identificado directamente, sin publicación de la resolución ni de los informes sustentatorios, y bajo causales amplias como seguridad, secreto militar u orden interno. En respuesta, consideramos imperativa una regla de cautela institucional: a mayor capacidad intrusiva de la tecnología, mayor debe ser la motivación, la trazabilidad, el control independiente y la posibilidad de revisión ex post.

Si el Estado considera indispensable adquirir tecnologías de esta naturaleza, la clasificación de la información podría proteger detalles operativos estrictamente necesarios, pero no debería bloquear toda información sobre existencia de la contratación, monto agregado, entidad adquirente, justificación general, controles aplicados y mecanismos de auditoría. Sin ello, la contratación secreta deja de ser una excepción funcional y se convierte en una zona de opacidad incompatible con una democracia constitucional.

TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y SPYWARE

1. PRINCIPIO DE PUBLICIDAD FRENTE A CULTURA DEL SECRETO

En el presente apartado analizaremos el régimen de excepciones al derecho de acceso a la información pública, no como un bloque aislado de normas administrativas, sino como el marco jurídico-constitucional que delimita cuándo el Estado puede cerrar información vinculada con vigilancia, inteligencia, orden interno y defensa nacional. Esta precisión es especialmente relevante para el análisis de spyware, pues la normativa de contratación pública puede decirnos cómo se adquiere una herramienta, pero la Ley de Transparencia y Acceso a la Información Pública (en adelante, la Ley de Transparencia o LTAIP) permite determinar qué información puede mantenerse legítimamente fuera del escrutinio público.

De acuerdo a ello, la Ley N.° 27806 (cuyo Texto Único Ordenado fue aprobado mediante Decreto Supremo N° 021-2019-JUS) parte de una regla general: todas las actividades y disposiciones de las entidades comprendidas en la ley se encuentran sometidas al principio de publicidad. Asimismo, dispone que toda información que posea el Estado

se presume pública, salvo las excepciones expresamente previstas en la ley, y que el Estado tiene la obligación de entregar la información solicitada en aplicación de dicho principio.

En buena cuenta, el punto de partida no es el secreto, sino la publicidad. El secreto es la excepción; la transparencia, la regla: allí donde el Estado pretenda reservar información sobre tecnologías de la vigilancia, como spyware, no basta con invocar seguridad nacional, inteligencia u orden interno de manera genérica. Debe demostrar que la información encaja estrictamente en una causal prevista en la ley, que su divulgación produciría un riesgo específico y que la restricción no encubre información que, por su naturaleza, debería permanecer accesible.

¿Cuál es la relevancia, entonces, de la Ley de Transparencia y Acceso a la Información Pública en el marco del presente informe sobre adquisición y uso de spyware? Nosotros identificamos dos funciones centrales. En primer lugar, la LTAIP permite encuadrar qué puede ser considerado secreto, reservado o confidencial cuando la Ley de Contrataciones habilita procedimientos no competitivos para bienes, servicios u obras declarados secretos, secretos militares o por razones de orden interno. Dicho de otro modo, orienta el ámbito de discrecionalidad administrativa para evitar que la clasificación se convierta en una decisión puramente política o funcional. En segundo lugar, la Ley de Transparencia permite identificar qué información, del ciclo de uso total (la negociación, su instalación, el despliegue, la recopilación de información, etcétera) del spyware, sí debería ser accesible (aún si el proceso de compra fuera secreto): protocolos generales, número de autorizaciones, criterios de control, auditorías, informes ex post, documentos no operativos o información sobre violaciones de derechos humanos.

En efecto, el Decreto Legislativo N.° 1129, que regula el Sistema de Defensa Nacional, establece de manera explícita en su artículo 12 que los acuerdos, actas, grabaciones, transcripciones y, en general, la información generada en asuntos de Seguridad y Defensa Nacional se rigen por la Ley de Transparencia y Acceso a la Información Pública en cuanto a difusión, acceso público y excepciones. De esta manera, incluso la

información vinculada con defensa y seguridad no se ubica fuera del régimen de transparencia, sino dentro de sus reglas de clasificación.

Así, la LTAIP opera como marco de interpretación de la reserva. Por ello, el análisis del uso y adquisición de spyware no puede quedarse en la pregunta "¿la entidad dijo que es secreto?", sino que debe formular una pregunta más exigente: ¿la información cumple los requisitos legales para ser secreta o reservada?

2. ANÁLISIS DE LAS EXCEPCIONES EN LA LEY DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA

2.1. Información secreta: ámbito militar e inteligencia

El artículo 15 de la Ley de Transparencia regula la información secreta. La norma establece que el derecho de acceso no puede ejercerse respecto de información expresamente clasificada como secreta, sustentada en razones de seguridad nacional, en concordancia con el artículo 163 de la Constitución, que tenga como base fundamental garantizar la seguridad de las personas y cuya revelación origine riesgo para la integridad territorial y/o la subsistencia del sistema democrático.

Esta redacción exige una lectura acumulativa. No basta con que la entidad invoque "seguridad nacional" para sustraer del acceso público cierta información. La clasificación secreta requiere, al menos:

1. Que exista una razón de seguridad nacional;
2. Que la clasificación tenga como base fundamental garantizar la seguridad de las personas;
3. Que la revelación genere un riesgo para la integridad territorial y/o la subsistencia del sistema democrático;
4. Que el supuesto encaje en alguno de los literales expresamente previstos por la ley.

En materia de spyware, el artículo 15 permite identificar dos ámbitos potencialmente relevantes.

a) Ámbito militar: En este ámbito, podrían ser relevantes las operaciones y planes de inteligencia y contrainteligencia militar, así como desarrollos técnicos o científicos propios de la defensa nacional. Sin embargo, esta posibilidad debe interpretarse de manera especialmente cerrada. El uso o adquisición de spyware no podría considerarse secreto por el solo hecho de involucrar a una institución militar o por tratarse de una tecnología sofisticada.

Para que esta información sea legítimamente secreta, debería encontrarse vinculada con defensa nacional en sentido estricto, esto es, con amenazas que comprometan la integridad territorial o la subsistencia del sistema democrático. En consecuencia, una persona sometida a vigilancia mediante spyware tendría que estar conectada, de manera jurídicamente sustentada, con una amenaza de esa magnitud. De lo contrario, la clasificación sería desproporcionada y potencialmente contra legem. El ámbito militar no convierte toda vigilancia en secreta: solo permite clasificar aquello que, por su contenido, finalidad y riesgo de divulgación, se conecte estrictamente con defensa nacional.

b) Ámbito de inteligencia: De otro lado, el artículo 15 también estipula que será clasificada como secreta la información relativa al ámbito de inteligencia, tanto en el frente externo como interno. Allí se incluyen, entre otros, los planes estratégicos y de inteligencia, la información que ponga en riesgo fuentes, informes cuya publicidad perjudicaría información de inteligencia, y actividades y planes estratégicos de inteligencia y contrainteligencia de los organismos del SINA.

Este es, sin duda, el ámbito más sensible para el análisis de spyware. La adquisición, despliegue o uso de spyware podría intentar encuadrarse como información secreta si se presenta como actividad de inteligencia o contrainteligencia del SINA. Sin embargo,

este razonamiento no puede hacerse de manera automática. La información debe estar vinculada con actividades reales del sistema de inteligencia, dentro del Estado de Derecho, y conforme a los supuestos expresamente contemplados por la ley.

La propia Ley del Sistema de Inteligencia Nacional refuerza esta conexión, al señalar que es información clasificada de inteligencia, con nivel de secreto, aquella que poseen o generan los componentes del SINA y que, por su naturaleza y contenido, constituye una excepción al acceso a información pública en razón de la seguridad nacional, de conformidad con la Ley de Transparencia. También considera clasificado el detalle de los recursos especiales asignados al SINA y las resoluciones que autorizan viajes al exterior de su personal.

No obstante lo anteriormente señalado, aquí aparece un problema jurídico importante. Como advierte León[49], la definición de información clasificada de inteligencia en el Decreto Legislativo N.° 1141 tiene un probable problema interpretativo de dimensión circular: se restringe porque es clasificada, y es clasificada porque constituye una excepción a la legislación de transparencia. La cláusula de inteligencia del artículo 15.2, al tener un enunciado tan amplio y abarcativo, es la más expuesta al abuso, precisamente porque puede ser utilizada para desplazar información sobre tecnologías de vigilancia fuera del escrutinio ciudadano.

2.2. Información reservada: orden interno y criminalidad, y acción externa del Estado

El artículo 16 regula la información reservada. Esta categoría comprende, principalmente, dos ámbitos: (i) orden interno y prevención o represión de la criminalidad; y (ii) relaciones externas del Estado.

a) Orden interno y prevención de criminalidad: La ley considera reservada la información cuya divulgación, por razones de seguridad nacional en el ámbito del orden interno, originaría un riesgo

[49] León Pacheco, Lucía. Loc. Cit.

para la integridad territorial y/o la subsistencia del sistema democrático. Asimismo, comprende información destinada a prevenir y reprimir la criminalidad cuya revelación podría entorpecer dicho fin.

Dentro de este grupo, los supuestos más relevantes en los referido a spyware son:

i. Planes de operaciones policiales y de inteligencia, incluidos aquellos destinados a combatir terrorismo, tráfico ilícito de drogas y organizaciones criminales.

ii. Informaciones que impidan el curso de investigaciones en etapa policial, incluyendo interceptación de comunicaciones amparadas por ley.

iii. Armamento y material logístico comprometido en operaciones especiales y planes de seguridad y defensa del orden interno.

Así, si el uso de spyware fuese entendido como herramienta de investigación policial, la entidad podría intentar sostener que determinada información vinculada está exenta del escrutinio público. Sin embargo, esta reserva no debería cubrir todo el universo informativo vinculado con la herramienta. La interpretación correcta debe distinguir entre:

1. Información cuya publicidad puede frustrar una operación específica o revelar una técnica operativa en curso;
2. Información institucional, estadística, contractual o normativa que permite fiscalizar el uso de la herramienta sin comprometer investigaciones concretas.

En efecto, no todo lo relacionado con el spyware en investigaciones penales debería ser reservado. Por ejemplo, en caso se use dicha herramienta tecnológica, una vez concluida una investigación o cuando ya no exista riesgo operativo, debería evaluarse el acceso a información agregada sobre cantidad de casos, tipos de delitos, número de autorizaciones, protocolos, controles aplicados, audito-

rías, entidades intervinientes y criterios de uso. Consideramos que la reserva por investigación no puede convertirse en reserva de política pública.

b) Relaciones externas del Estado: El artículo 16.2 también contempla información reservada por razones de seguridad nacional y eficacia de la acción externa del Estado. En este ámbito podrían encajar, en ciertos casos, negociaciones internacionales o acuerdos Estado-Estado vinculados con adquisición, cooperación, asistencia técnica o intercambio de capacidades de vigilancia.

Sin embargo, esta causal también debe interpretarse taxativamente. Solo podría reservarse aquello cuya revelación afecte el curso de negociaciones internacionales, relaciones diplomáticas, defensa nacional en el frente externo o la subsistencia del sistema democrático. En consecuencia, no toda compra a proveedor extranjero, ni todo convenio internacional de seguridad, quedan automáticamente reservados.

De esta forma, la participación de un proveedor extranjero o de otro Estado no transforma por sí sola la adquisición de spyware en información reservada. La entidad debe demostrar el daño específico que produciría la divulgación. Además, queda la pregunta pública sobre la legitimidad de un Estado que se vincula y/o negocia de forma directa con otro Estado respecto de una tecnología tan altamente intrusiva y potencialmente peligrosa para los derechos humanos.

2.3. Información confidencial: deliberación y secreto comercial

De otro lado, el artículo 17 regula la información confidencial. Aunque el objetivo final del spyware suele concentrarse en secreto y reserva, la confidencialidad también puede aparecer en la adquisición de estas herramientas, especialmente por dos vías:

1. **Consejos, recomendaciones u opiniones previas a una decisión gubernamental.**

   Podría alegarse confidencialidad respecto de informes internos previos a la decisión de adquisición. Sin embargo, esta protección no debería subsistir indefinidamente ni cubrir la motivación final de la decisión administrativa.

2. **Secreto comercial o industrial.**

   Los proveedores de spyware podrían alegar confidencialidad sobre código fuente, arquitectura técnica, exploits, infraestructura, precios unitarios, licencias o condiciones comerciales. Sin embargo, el secreto comercial no puede desplazar el interés público en conocer la existencia de la contratación, el monto global, la entidad adquirente, el objeto general, las salvaguardas contractuales y los mecanismos de control.

De acuerdo a ello, entendemos que la información confidencial debe operar mediante reserva parcial y no como bloqueo integral del expediente. Así, si un contrato de spyware contiene secretos comerciales, corresponde tachar o disociar aquello estrictamente protegido, no excluir del ámbito público toda la información que podría estar vinculado a ello.

3. INTERPRETACIÓN RESTRICTIVA Y VIOLACIONES A LOS DERECHOS HUMANOS

Es importante recalcar una máxima en torno al uso de las excepciones: estas deben interpretarse de manera restrictiva. El artículo 18 establece que las excepciones de los artículos 15, 16 y 17 son las únicas que pueden limitar el derecho de acceso, precisamente porque se trata de una restricción a un derecho fundamental.

Asimismo, el artículo 18 contiene una regla especialmente importante para la problemática de spyware: no se considera información clasificada aquella relacionada con violaciones de derechos humanos o de los

Convenios de Ginebra de 1949, en cualquier circunstancia y por cualquier persona. Esta regla es importante porque si el uso de spyware constituye vigilancia abusiva, persecución de periodistas, vigilancia de defensores, interceptación ilegal, afectación masiva de derechos o uso contra personas sin base legal, la información relativa a tales hechos no debería quedar protegida por secreto, reserva o confidencialidad, en tanto implicarían, por sí mismas, violaciones a los derechos humanos.

Nosotros sostenemos que el spyware, por su propia arquitectura intrusiva, produce riesgos casi intolerables para los derechos fundamentales. Por tanto, su uso abusivo, ilegal, desproporcionado o dirigido contra sociedad civil, periodistas, opositores o defensores de derechos puede constituir una violación de derechos humanos y, por tanto, no alcanza, bajo ningún supuesto, el paraguas de clasificación de la información relacionada.

4. PLAZOS DE CLASIFICACIÓN: RÉGIMEN COMÚN, RÉGIMEN DE INTELIGENCIA Y PROBLEMA DE ASIMETRÍA

El régimen temporal de clasificación de información también revela una tensión importante. Podríamos identificar que existen dos regímenes: uno común y uno (o unos) especiales. El primero, regulado en la LTAIP; y, el segundo, regulado en las leyes especiales (como del sistema de inteligencia). En el régimen común de la LTAIP, la información secreta puede ser solicitada después de cinco años de su clasificación. La entidad deberá entregarla si su divulgación no pone en riesgo la seguridad de las personas, la integridad territorial o la subsistencia del sistema democrático. Si decide mantener la clasificación, debe fundamentarlo expresamente y por escrito, y el documento que sostiene la continuidad de la reserva debe ponerse en conocimiento del Consejo de Ministros y de la comisión parlamentaria correspondiente.

No obstante ello, la información producida por el Sistema de Inteligencia Nacional tiene un régimen especial. El Decreto Legislativo N.° 1141 establece que la desclasificación de información clasificada producida

por el SINA, relativa a seguridad nacional, procede a los veinte años. Luego de ese plazo, cualquier ciudadano peruano puede solicitarla, pero su entrega depende de que el titular del sector o pliego, con opinión favorable del Director de Inteligencia Nacional, considere que su divulgación no genera riesgo para la seguridad de las personas, la integridad territorial o la subsistencia del sistema democrático.

Este desfase es relevante: cinco años en el régimen común; veinte años en el régimen de inteligencia. León[50] advierte que esta diferencia agrava los problemas de transparencia, pues el periodo de clasificación en inteligencia es mucho mayor que el régimen común, y ello se combina con una definición circular de información clasificada de inteligencia.

Así, el uso de spyware bajo cobertura del SINA genera un riesgo particular: la información puede quedar bloqueada durante un periodo excesivamente largo, aun cuando el interés público en conocer la adquisición, despliegue o abuso de estas herramientas sea especialmente alto. En consecuencia, el tiempo también puede configurarse como una forma de opacidad: si la información sobre spyware se libera veinte años después, la posibilidad de control democrático, sanción o reparación puede llegar demasiado tarde (o nunca llegar del todo).

5. VIGILANCIA Y CLASIFICACIÓN DE INFORMACIÓN: QUÉ NO SE PODRÍA CLASIFICAR

De lo expuesto hasta este punto, sostenemos que, como principio y garantía democrática, en materia de vigilancia, en general, y uso de spyware, en particular, no podría considerarse clasificada:

1. La existencia de políticas o protocolos generales sobre adquisición y uso de spyware;
2. El monto global de adquisición;
3. La entidad adquirente;

[50] Ibidem.

4. La existencia de contratos, convenios o adquisiciones, al menos en versión pública;
5. Los criterios generales de necesidad y proporcionalidad para su uso;
6. Los mecanismos de autorización y control;
7. Estadísticas agregadas sobre uso;
8. Auditorías ex post, cuando no comprometan operaciones concretas;
9. Información relativa a usos abusivos o violaciones de derechos humanos.

Así, sostenemos que el secreto podría proteger el "cómo operativo" de una medida legítima, pero no debería borrar el "si existe", "quién decide", "con qué controles", "por cuánto" y "con qué límites".

En resumen, somos de la opinión que el Estado puede proteger información sensible vinculada con defensa, inteligencia y orden interno. Sin embargo, esa protección debe operar bajo criterios estrictos, controlables y temporales. No obstante ello, en lo referido a tecnologías de la vigilancia altamente intrusivas (como spyware), se tensiona el sistema porque suele ubicarse justamente en las zonas más opacas del aparato estatal: seguridad, inteligencia, criminalidad organizada y cooperación internacional.

En buena cuenta, consideramos como regla básica, en caso se use spyware u otra tecnología de vigilancia similar (suponiendo su legalidad y proporcionalidad): solo debe restringirse el acceso a información cuando la entidad demuestre, de manera concreta, que la información encaja en una causal legal, que su divulgación genera un riesgo real y que no existe una forma menos restrictiva de entregar acceso parcial o agregado. Todo lo demás, especialmente cuando involucra violaciones de derechos humanos, debe permanecer bajo control público e institucional.

SISTEMA DE INTELIGENCIA NACIONAL Y USO DE SPYWARE

1. LA INTELIGENCIA Y EL PRINCIPIO DE LEGITIMIDAD: SEGURIDAD NACIONAL, DERECHOS FUNDAMENTALES Y LEGALIDAD

En este apartado corresponde analizar el régimen del Sistema de Inteligencia Nacional porque buena parte de las excepciones previamente revisadas, tanto en materia de contrataciones públicas como en materia de acceso a la información, remiten directa o indirectamente al ámbito de la inteligencia, la contrainteligencia, la seguridad nacional, el orden interno o la defensa nacional.

Esta remisión no es menor. En efecto, la Ley N.° 32069 permite contrataciones no competitivas de las Fuerzas Armadas, la Policía Nacional del Perú y los componentes del SINA cuando hayan sido declaradas de carácter secreto, secreto militar o por razones de orden interno. A su vez, la Ley de Transparencia y Acceso a la Información Pública reconoce excepciones vinculadas con información secreta y reservada en materia militar, policial y de inteligencia. El Decreto Legislativo N.° 1141, por su lado, define los

principios, límites, controles y procedimientos que permiten determinar cuándo una actividad puede ser considerada inteligencia legítima y cuándo, por el contrario, se trata de una actuación estatal fuera del marco legal.

¿Significa ello que toda información vinculada al SINA queda automáticamente excluida del acceso público? Entendemos que no. La inteligencia puede requerir reserva, pero la reserva no convierte a la inteligencia en una zona inmune al Derecho. En buena cuenta, la clasificación de información solo puede proteger actividades de inteligencia realizadas dentro del marco convencional, constitucional y legal aplicable.

En esta línea, el artículo 3, inciso 2, del Decreto Legislativo N.° 1141 establece que las actividades de inteligencia se legitiman en razón de la seguridad nacional, "respetando el equilibrio entre las necesidades del Estado y los derechos de las personas y el respeto a la ley". Esta fórmula es central en materia de vigilancia digital porque impide entender la seguridad nacional como una habilitación ilimitada para acceder a dispositivos, comunicaciones o datos personales.

De acuerdo a ello, es posible identificar tres elementos materiales del principio de legitimidad:

1. **Finalidad constitucionalmente relevante.** La actividad de inteligencia debe estar orientada a la seguridad nacional y no a fines políticos, personales, discriminatorios o de control indebido de la sociedad civil.
2. **Respeto de los derechos de las personas.** La inteligencia no puede ejercerse desconociendo privacidad, inviolabilidad de comunicaciones, datos personales, libertad de expresión, asociación, defensa legal o integridad personal.
3. **Sujeción estricta a la ley.** La actividad debe realizarse conforme a procedimientos, autorizaciones, límites y controles previstos por el ordenamiento jurídico.

Asimismo, el artículo 4 del Reglamento del Decreto Legislativo N.° 1141 refuerza esta idea al establecer que la autorización y ejecución de actividades de inteligencia debe realizarse en estricto cumplimiento de la Constitución, las leyes, los principios de inteligencia y el respeto de los derechos humanos. Además, prohíbe que los componentes del SINA produzcan inteligencia o ejecuten medidas de contrainteligencia para propósitos distintos a garantizar la vigencia de los derechos humanos, defender la soberanía nacional, promover el bienestar general, proteger a la población frente a amenazas contra su seguridad, o por razones discriminatorias como origen, raza, sexo, idioma, religión, opinión, condición económica u otra índole.

En buena cuenta, el SINA no tiene una carta blanca para vigilar. Su legitimidad depende de que la actividad de inteligencia se mantenga dentro de una finalidad constitucionalmente válida, bajo límites materiales y con respeto efectivo de derechos fundamentales.

2. MECANISMOS DE CONTROL DE LA ACTIVIDAD DE INTELIGENCIA FRENTE AL USO DE SPYWARE

2.1. Control judicial

La ley establece un mecanismo de control judicial para el supuesto de un uso operativo de spyware en inteligencia: los procedimientos especiales de obtención de información. El Reglamento, en su artículo 11.3, exige que para autorizar planes de inteligencia y contrainteligencia se verifique la posible limitación o restricción de derechos fundamentales, en cuyo caso debe seguirse el procedimiento especial de obtención de información. Es decir, si el plan de inteligencia implica limitar o restringir derechos fundamentales, se debería acudir a este tipo de procedimiento.

El artículo 32.1 del Decreto Legislativo N.° 1141 establece que estos procedimientos son ejecutados exclusivamente por los componentes del

SINA y se utilizan para acceder a información estrictamente indispensable para cumplir los objetivos de la actividad de inteligencia. Esta regla contiene un estándar especialmente exigente: la información debe ser estrictamente indispensable. No basta que sea útil, conveniente, interesante o potencialmente valiosa. Debe ser necesaria en un sentido reforzado para la finalidad de inteligencia. En este sentido, el artículo 32.2 del Decreto Legislativo N.° 1141 establece que su ejecución requiere autorización judicial otorgada por cualquiera de los dos jueces superiores ad hoc designados por la Corte Suprema. Además, dispone que todo el proceso constituye información clasificada como secreta.

El artículo 33.1 precisa que la solicitud de autorización solo puede ser presentada por el Director de Inteligencia Nacional y debe contener: 1) Identificación de la persona o personas afectadas; 2) Especificación de las medidas solicitadas; y, 3) Motivación y duración de dichas medidas. Así, si el software de espionaje fuese utilizado como mecanismo de obtención de información en inteligencia que afecte derechos fundamentales, su uso debería pasar, como mínimo, por este procedimiento especial, que habilita el control judicial de la actividad de inteligencia.

Así, podemos concluir que la ley no permite un uso informal, genérico o exploratorio de herramientas intrusivas. Si la medida afecta derechos fundamentales, debe existir control judicial. Y si la tecnología es spyware, por su intensidad intrusiva, la afectación de derechos no es una posibilidad remota, sino el centro mismo de su funcionamiento por lo que, en caso se use para actividades de inteligencia, debe contar con autorización judicial en todos los supuestos.

Ahora bien, el artículo 33.5 del Decreto Legislativo N° 1141 regula un supuesto excepcional: en caso de peligro contra la seguridad nacional y por la urgencia de las circunstancias, el Director de Inteligencia Nacional puede autorizar la ejecución de un procedimiento especial de obtención de información, con cargo a formalizar de inmediato la solicitud ante el juez superior ad hoc, quien en veinticuatro horas puede convalidarlo o disponer su inmediata paralización.

Esta regla, al ser una excepción, debe interpretarse restrictivamente. La urgencia no puede convertirse en un sustituto ordinario de la autorización judicial previa. En efecto, estamos ante una excepción dentro de un régimen ya excepcional: primero, porque se trata de inteligencia; segundo, porque se trata de procedimientos especiales de obtención de información; tercero, porque se permite iniciar la medida antes del control judicial.

De acuerdo a ello, nosotros entendemos que el uso urgente de spyware solo podría considerarse admisible, en términos abstractos, si concurren acumulativamente: a) peligro concreto contra la seguridad nacional; b) urgencia real e impostergable; y, c) imposibilidad material de obtener autorización previa sin frustrar la finalidad legítima. En buena cuenta, la urgencia no borra el control judicial: solo lo desplaza temporalmente, bajo una carga reforzada de motivación.

2.2. Valor probatorio de los informes de inteligencia y límites frente al proceso penal

El artículo 34 del Decreto Legislativo N.° 1141 establece que, en ningún caso, los informes de inteligencia tienen valor probatorio dentro de procesos judiciales, administrativos o disciplinarios; sin embargo, su contenido puede constituir elemento orientador durante la investigación. Esta regla es relevante porque impide que la inteligencia sea trasladada mecánicamente al proceso como prueba. Si el spyware se utiliza en el ámbito de inteligencia, la información obtenida no debería ingresar directamente como prueba, sino, en todo caso, orientar una investigación que deberá producir evidencia conforme a las reglas procesales correspondientes.

Esta disposición busca preservar una separación mínima entre inteligencia y prueba. Sin embargo, también abre una zona gris: si la inteligencia obtenida mediante software espía orienta una investigación penal posterior, debe existir un mecanismo que permita controlar que la investigación no se construyó sobre una fuente ilícita, desproporcionada o no autorizada. Si la información sobre inteligencia se mantiene

como clasificada, ¿Cómo podría la persona involucrada en un proceso o procedimiento cuestionar que se usa inteligencia como prueba? Además, ¿Cómo cuestionar que únicamente se usa como elemento orientador si no se accede o se puede conocer esta actividad de inteligencia?

En buena cuenta, que un informe de inteligencia no tenga valor probatorio no elimina el riesgo de contaminación del proceso. Si la información originaria fue obtenida ilegalmente, su uso como "orientación" también debería ser objeto de control. Y, cuando hablamos de spyware, la persona que ha sido objeto de su uso debería ser notificada y puesta en conocimiento de ello para poder tener herramientas y ejercer adecuadamente su derecho de defensa.

2.3. Destrucción obligatoria de información innecesaria y derechos fundamentales

El artículo 35 del Decreto Legislativo N.° 1141 establece una regla particularmente importante para el análisis de spyware: toda información obtenida para la producción de inteligencia por el SINA que sea innecesaria para el objetivo del sistema, por corresponder a derechos fundamentales de la persona humana y a la esfera de su vida privada, debe ser destruida por los funcionarios responsables, bajo responsabilidad de inhabilitación y sin perjuicio de sanciones civiles o penales. Esta disposición revela que el propio régimen de inteligencia reconoce que puede obtenerse información que comprometa derechos fundamentales y vida privada, pero ordena su destrucción cuando sea innecesaria para los objetivos del sistema.

De acuerdo a ello, en lo que aquí respecta, esta regla adquiere una relevancia especial. Dado que el spyware puede capturar información masiva, íntima y colateral, incluyendo datos de terceros no investigados, conversaciones personales, fotografías, archivos, contactos o comunicaciones protegidas, el deber de destrucción debería operar como una garantía mínima de minimización y depuración.

No obstante ello, esta garantía plantea un problema práctico: ¿Cómo puede verificarse que la información innecesaria fue destruida si todo el procedimiento está clasificado? Para poder dar una solución objetiva y viable, deben existir registros, trazabilidad, auditorías internas, control judicial y control institucional posterior que permitan verificar, al menos ante órganos competentes, que la destrucción ocurrió. Si el Estado usa herramientas capaces de absorber la vida digital de una persona, debe poder demostrar que eliminó aquello que no tenía derecho a conservar.

3. RECURSOS ESPECIALES Y CONTRATACIONES RESERVADAS: UNA ZONA DE OPACIDAD REFORZADA

El Decreto Legislativo N.° 1141 también regula los llamados recursos especiales. El artículo 30.1 los define como aquellos destinados a atender gastos de naturaleza reservada de la actividad de inteligencia que, de hacerse públicos, pondrían en riesgo la seguridad nacional, la integridad del personal de inteligencia o sus fuentes de información. Además, prohíbe destinarlos a aumentos, pagos ordinarios o gastos personales del personal de la DINI o de los componentes del SINA. Sobre ello, el artículo 31 establece que las contrataciones con cargo a recursos especiales, las fuentes de información o la integridad del personal del SINA, tienen clasificación de secreto.

Creemos que sí es razonable que existan mecanismos reservados para gastos estrictamente vinculados con inteligencia. Sin embargo, esta reserva plantea una zona de especial preocupación cuando se trata de spyware. En efecto, una herramienta de vigilancia digital altamente intrusiva podría ser adquirida con cargo a recursos especiales, bajo clasificación secreta y sin publicidad ordinaria del proceso contractual.

4. INTELIGENCIA Y LEGALIDAD COMO REQUISITO DE CLASIFICACIÓN DE INFORMACIÓN LEGÍTIMA

El artículo 4.1 del Decreto Legislativo N.° 1141 establece que es información clasificada de inteligencia, con nivel de secreto, aquella que poseen o generan los componentes del SINA y que, por su naturaleza y contenido, constituye una excepción al derecho de acceso a la información pública en razón de la seguridad nacional, conforme a la Ley de Transparencia y Acceso a la Información Pública. Esta redacción es importante por una razón: la clasificación no deriva únicamente del sujeto que posee la información, sino también de su naturaleza, contenido y encaje en las excepciones de la LTAIP. Dicho de otro modo, no toda información en manos del SINA es secreta per se. Para que la clasificación sea válida, debe cumplir con los supuestos materiales previstos por la LTAIP.

Adicionalmente, como pudimos observar de lo hasta aquí desarrollado, la ley estipula limitaciones y garantías de control de la actividad de inteligencia. En efecto, recordemos que la legitimidad de la actividad de inteligencia se deriva de la seguridad nacional siempre que se respete el equilibrio entre las necesidades del Estado y los derechos de las personas y el respeto a la ley. Es decir, no hay actividad legítima de inteligencia si no se ponderan los intereses del Estado, los derechos fundamentales y la legalidad de la actuación.

De acuerdo con ello, sostenemos que la clasificación de información vinculada con inteligencia, para ser legal y gozar de todas las prerrogativas de la clasificación, debe superar dos niveles de análisis jurídico.

I. Encaje formal en la LTAIP: No toda información de inteligencia es secreta o reservada por el solo hecho de provenir del SINA. Debe encajar taxativamente en los supuestos de la LTAIP, ya sea como información secreta, reservada o confidencial. En consecuencia, la entidad debe justificar por qué su divulgación pondría en riesgo seguridad nacional, fuentes, operaciones, integridad territorial, subsistencia del sistema democrático u otros bienes expresamente protegidos.

II. Conformidad material con el Decreto Legislativo N° 1141: Además del encaje formal, la actividad que generó la información debe haber sido realizada conforme a los límites materiales del sistema de inteligencia. Esto implica:

1. Finalidad legítima de seguridad nacional;
2. Respeto de derechos humanos;
3. Prohibición de fines discriminatorios o ajenos a los objetivos del SINA;
4. La actividad de inteligencia debe estar prevista en Plan de Inteligencia Nacional (PIN) y en los Planes Institucionales de Inteligencia (PII) de cada organismo del sistema;
5. Evaluación de riesgos de la actividad de inteligencia y, en caso se ponga en riesgo derechos fundamentales, ejecutar mediante procedimientos especiales;
6. Autorización judicial cuando se trate de procedimientos especiales con motivación, duración e identificación de personas afectadas;
7. Destrucción de información innecesaria;
8. Cumplir con el control institucional correspondiente (opinión favorable previa de la Contraloría General de la República para recursos especiales e información permanente a la Comisión de Inteligencia del Congreso).

De esta manera, la clasificación solo conserva legitimidad si protege una actividad de inteligencia desarrollada dentro del Derecho. Si la actividad es ilegal, abusiva o contraria a derechos fundamentales, la clasificación pierde su fundamento y debe habilitarse el control ciudadano, sin perjuicio del control institucional, judicial o parlamentario.

En buena cuenta, la clasificación no puede proteger información generada por una actuación de inteligencia ilícita. Si la actividad material se aparta de la ley, la reserva debería perder su fundamento constitucional en la medida que solo la inteligencia legal merece reserva. La inteligencia ilegal no puede reclamar los privilegios del secreto y, por tanto, el escrutinio ciudadano, además del institucional, queda habilitado.

5. INFORMACIÓN DE INTELIGENCIA SOBRE SPYWARE QUE DEBERÍA SER ACCESIBLE

En la medida que no toda actividad de inteligencia es, por sí misma, clasificada, reiteramos, conforme a lo que expuesto previamente, que sí existe un ámbito de control ciudadano que podría exigirse sobre la utilización de spyware (o al menos mediante acceso público parcial o versiones agregadas), a saber:

1. Existencia de protocolos generales para el uso de spyware;
2. Criterios de autorización judicial;
3. Número agregado de solicitudes y autorizaciones;
4. Duración promedio de medidas;
5. Mecanismos de destrucción de información innecesaria;
6. Existencia de auditorías o controles;
7. Montos globales de adquisición, salvo justificación excepcional;
8. Entidad responsable de la adquisición;
9. Información sobre usos abusivos, ilegales o violatorios de derechos humanos.

En buena cuenta, la clasificación puede proteger el detalle operativo legítimo, pero no debería impedir conocer si el Estado cuenta con spyware, bajo qué reglas generales lo usa, qué controles aplica y qué mecanismos existen para reparar abusos.

¿VIABILIDAD CONSTITUCIONAL DEL SPYWARE EN EL PERÚ?

Finalmente, el análisis del régimen de inteligencia nos conduce a una pregunta inevitable: ¿puede el uso de spyware ser proporcional o admisible dentro de una actividad de inteligencia constitucionalmente válida?

La respuesta no puede ser automática. Consideramos que, por su naturaleza, el software de espionaje representa una de las formas más intensas de afectación de derechos fundamentales, pues puede acceder al conjunto de comunicaciones, datos, imágenes, ubicación, contactos, archivos y sensores de un dispositivo. Por tanto, cualquier uso estatal de esta tecnología debe superar un estándar especialmente estricto de legalidad, finalidad, necesidad, proporcionalidad, autorización judicial y trazabilidad.

Así, el siguiente nivel de análisis consiste en responder si el spyware puede ser constitucional bajo algún supuesto. Y esa pregunta exige evaluar si una tecnología diseñada para infiltrarse en la vida digital completa de una persona puede superar, en algún caso, el test de legalidad, necesidad y proporcionalidad dentro de una democracia constitucional.

Por lo tanto, en este apartado trataremos de dar respuesta a la pregunta más compleja del presente reporte: ¿puede el Estado usar spyware de manera constitucionalmente admisible? La pregunta no es menor porque el software espía no opera como una simple herramienta de monitoreo externo, ni como una técnica tradicional de vigilancia sobre una comunicación específica. Como lo mencionamos previamente, consideramos que el spyware constituye una medida de vigilancia de intensidad máxima, pues no se limita a intervenir una comunicación concreta, sino que compromete el entorno digital completo de una persona.

Dicho de otro modo, si la interceptación clásica afecta una comunicación, el spyware afecta el dispositivo desde el cual se desarrollan múltiples dimensiones de la vida privada, comunicacional, profesional, familiar, política y asociativa. El spyware no es una técnica más dentro del catálogo de vigilancia estatal; es una tecnología que, por su diseño, acumula varias capacidades de vigilancia en una sola intrusión.

1. LA EXIGENCIA CONSTITUCIONAL DE ORDEN JUDICIAL

A partir de lo anteriormente desarollado, la primera consecuencia constitucional es clara: en la medida en que el spyware permite acceder a comunicaciones, documentos privados y datos personales, su eventual uso estatal requeriría, como mínimo, orden judicial previa, motivada y específica.

Esta exigencia se desprende de la Constitución peruana, particularmente del artículo 2, inciso 10, que reconoce el secreto e inviolabilidad de las comunicaciones y documentos privados, y establece que estos solo pueden ser abiertos, incautados, interceptados o intervenidos por mandato motivado del juez, con las garantías previstas en la ley. A ello se suma la afectación de la vida privada, la intimidad, la autodeterminación informativa, el debido proceso, la libertad de expresión, entre otros,mencionados previamente.

De acuerdo a ello, una primera conclusión a la que llegamos es que cualquier uso de spyware sin orden judicial es constitucionalmente inadmisible. No se trataría de una irregularidad menor o subsanable ex post, sino de una intervención directa sobre el núcleo de derechos fundamentales que la Constitución somete expresamente a control judicial.

Así, si una tecnología permite ingresar al dispositivo de una persona, capturar comunicaciones y acceder a documentos privados, no puede ser tratada solamente como una mera herramienta administrativa-policial de monitoreo, patrullaje o inteligencia informal. Su punto mínimo de legitimidad es la autorización judicial. Por ello, descartaremos, a continuación, algunas vías que por su creciente uso en entornos digitales podrían intentar presentarse como supuestos habilitantes para el uso de spyware.

a) Agentes encubiertos y agentes virtuales: León[51] explica que el Código Procesal Penal prevé técnicas especiales de investigación, reguladas principalmente en el artículo 341, y que inicialmente el artículo trataba sobre agentes encubiertos, pero luego amplió su alcance hacia nuevas figuras, incluyendo agentes en entornos digitales. Sostenemos que estas figuras no pueden habilitar el uso de *spyware*. Un agente encubierto, incluso en entornos digitales, puede interactuar, observar, infiltrarse comunicacionalmente o participar bajo identidad encubierta en determinados espacios de investigación. No obstante, ello no equivale a tomar control remoto de un dispositivo, acceder a archivos privados, extraer comunicaciones cifradas o activar sensores del equipo.

En buena cuenta, la figura del agente encubierto permite ocultar identidad funcional; no permite invadir la totalidad del dispositivo de una persona. Usarla como cobertura para spyware sería una expansión contra legem de una técnica especial de investigación.

[51] Íbid.

b) Patrullaje virtual y monitoreo policial digital: De otro lado, tampoco podría justificarse el uso de spyware bajo categorías de patrullaje virtual, ciberpatrullaje o monitoreo de redes. Estas prácticas, incluso cuando se reconocen en normas sectoriales o policiales[52], se orientan principalmente a la observación de entornos digitales, fuentes abiertas, plataformas o interacciones visibles. En cambio, el spyware opera sobre información no pública, protegida constitucionalmente y alojada dentro del dispositivo.

La diferencia es sustantiva: una cosa es monitorear publicaciones abiertas en redes sociales, con todos los problemas que ello ya genera; y, otra muy distinta es infiltrarse en un teléfono para acceder a mensajes, fotografías, contactos, ubicación y aplicaciones privadas. Podríamos decir que el "patrullaje virtual" mira la "calle digital"; mientras que el spyware entra a la "casa digital". Y para entrar a la casa, constitucionalmente, se necesita una orden judicial.

Por todo ello, el uso de spyware queda descartado como herramienta ordinaria de vigilancia estatal, patrullaje digital, prevención general o inteligencia policial. Si alguna vez pudiera ser jurídicamente admisible, solo podría serlo dentro de procesos que cuenten con orden judicial y garantías reforzadas.

2. LOS DOS ÚNICOS MARCOS NORMATIVOS POSIBLES: PROCESO PENAL E INTELIGENCIA

Si el punto mínimo de legitimidad es la orden judicial, el marco peruano solo deja dos posibles vías normativas para discutir, en abstracto, un eventual uso de spyware: el proceso penal y el procedimiento especial de inteligencia. Fuera de estas dos vías, no existe un marco normativo que permita siquiera iniciar una discusión seria sobre el uso estatal de software de espionaje. Y aun dentro de ellas, como veremos, el marco vigente es insuficiente.

[52] Íb.

2.1. El artículo 230 del Código Procesal Penal: habilitación judicial, pero insuficiente para spyware

El artículo 230 del Código Procesal Penal se refiere a la intervención, grabación o registro de comunicaciones telefónicas u otras formas de comunicación, así como geolocalización de teléfonos móviles. Este permite que el fiscal, por iniciativa propia o a requerimiento de la Policía Nacional, solicite al juez de investigación preparatoria la intervención, monitoreo o grabación de comunicaciones telefónicas, radiales, por Internet u otras formas de comunicación, así como los registros de datos derivados de las comunicaciones, cuando existan suficientes elementos de convicción sobre un delito sancionado con pena superior a cuatro años y la medida sea absolutamente necesaria para proseguir la investigación.

Esta habilitación en la intrusión de los derechos fundamentales contiene algunos elementos relevantes:

1. Exige suficientes elementos de convicción;
2. Exige delito sancionado con pena superior a cuatro años;
3. Exige necesidad absoluta para continuar la investigación;
4. Requiere autorización judicial;
5. Debe identificar, cuando sea posible, a la persona afectada y el medio intervenido;
6. Debe indicar forma, alcance y duración de la medida;
7. Limita la duración a sesenta días, prorrogables por igual plazo y por única vez;
8. Prevé registro, actas, conservación, notificación posterior y reexamen judicial conforme al artículo 231.

No obstante las garantías enunciadas, consideramos que sus presupuestos son insuficientes para habilitar el uso de spyware por las siguientes razones:

a) Umbral delictivo excesivamente amplio

El primer problema es el umbral penal. La norma permite la intervención respecto de delitos sancionados con pena superior a cuatro años. Para una técnica tradicional de interceptación de comunicaciones, este umbral ya exige discusión. Para spyware, resulta claramente insuficiente. Recordemos que este software no interviene únicamente una llamada o una comunicación concreta, sino que puede irrumpir en el universo digital de una persona. Por ello, la gravedad del delito habilitante debería ser mucho más estricta, taxativa y excepcional. No bastaría una pena superior a cuatro años, pues ese criterio comprende un catálogo demasiado amplio de delitos.

De acuerdo a ello, si el spyware fuese discutido dentro del proceso penal, su uso debería limitarse, como mínimo, a delitos extremadamente graves, definidos de forma taxativa y vinculados con amenazas intensas a bienes jurídicos fundamentales, no a cualquier delito que supere un umbral punitivo relativamente bajo. En buena cuenta, el estándar de cuatro años puede servir para ciertas intervenciones de comunicaciones, pero no para una tecnología que puede convertir un teléfono entero en fuente total de vigilancia.

b) La norma regula comunicaciones, no toma de control del dispositivo

El segundo problema es el objeto de la medida. El artículo 230 regula intervención, monitoreo o grabación de comunicaciones y geolocalización. Aunque menciona Internet y otras formas de comunicación, su centro normativo sigue siendo la comunicación y los datos derivados de esta.

El software espía, en cambio, puede acceder a archivos que no son solo comunicaciones, sino también fotografías, notas, credenciales, historial, documentos, contactos, aplicaciones, cámaras, micrófonos y otros datos almacenados o generados por el dispositivo. Por lo tanto, pretender subsumirlo sin más en el artículo 230 genera un problema de legalidad: el artículo 230 autoriza intervenir comunicaciones; no autoriza intervenir la vida digital completa. Y, cuando una técnica supera cualitativamente el supuesto previsto por la norma, no corresponde ampliarla por analogía en perjuicio de derechos fundamentales (por principios de interpretación constitucional).

c) Falta de garantías técnicas específicas

El tercer problema es la ausencia de garantías técnicas adaptadas al spyware. Los artículos 230 y 231 regulan duración, registro, actas, conservación, notificación y reexamen. Sin embargo, no establecen reglas específicas sobre, por ejemplo: instalación o desinstalación de software intrusivo; límites de acceso a carpetas, aplicaciones o sensores; prohibición de alterar datos; registro técnico de cada acceso realizado; control de integridad forense; minimización de datos de terceros; cadena de custodia digital reforzada; entre otros.

Esta ausencia es especialmente grave porque el spyware puede modificar, extraer o generar datos dentro del dispositivo. En consecuencia, el riesgo no es solo que se obtenga información privada, sino que se afecte la integridad de la evidencia o se contamine la investigación penal. En buena cuenta, el Código Procesal Penal regula una diligencia de intervención específica; el spyware exige un régimen completo de intrusión digital forense.

d) Notificación y reexamen debilitados

El artículo 231 prevé que, una vez ejecutada la medida y realizadas las investigaciones inmediatas, se ponga en conocimiento del afectado todo lo actuado, quien puede solicitar reexamen judicial. Sin embargo, esta notificación solo será posible si el objeto de la

investigación lo permite y si no pone en peligro la vida o integridad de terceras personas.

Tratándose de spyware, esta regla resulta insuficiente si no se establecen plazos máximos, supuestos estrictos para diferir la notificación y obligación de informar, al menos ex post, el tipo de intrusión sufrida. Sin notificación posterior, no hay reexamen real; sin reexamen real, no hay remedio efectivo; sin remedio efectivo, la autorización judicial inicial se vuelve el único punto de control, y eso es demasiado poco para una tecnología de esta intensidad.

2.2. Procedimientos especiales de inteligencia

De otro lado, el Decreto Legislativo N.° 1141 regula los procedimientos especiales de obtención de información. El artículo 32 establece que estos procedimientos son ejecutados exclusivamente por los componentes del SINA y se utilizan cuando la actividad de inteligencia afecta los derechos fundamentales; esto, en miras a acceder a información estrictamente indispensable para cumplir los objetivos de la actividad de inteligencia. Además, requieren autorización judicial de jueces superiores ad hoc, y todo el proceso constituye información clasificada como secreta.

El artículo 33 exige que la solicitud sea presentada por el Director de Inteligencia Nacional y contenga identificación de las personas afectadas, especificación de las medidas solicitadas, motivación y duración. Asimismo, regula una excepción de urgencia, bajo la cual el Director puede autorizar provisionalmente la medida en caso de peligro contra la seguridad nacional y urgencia, con cargo a formalizar de inmediato ante el juez ad hoc.

No obstante ello, consideramos que el régimen de procedimientos especiales del SINA tampoco cuenta con las salvaguardas adecuadas, por las siguientes razones:

a) "Objetivos de inteligencia", supuesto demasiado amplio

El problema central es la amplitud del enunciado normativo habilitante. La norma permite procedimientos especiales para acceder a información estrictamente indispensable para el cumplimiento de "los objetivos de la actividad de inteligencia". Esta disposición es muy amplia y hace que el estándar de control judicial pierda fuerza.

De acuerdo a ello, sostenemos que el uso de spyware no podría habilitarse para cualquier objetivo de inteligencia. Debería limitarse a supuestos excepcionales de seguridad nacional demostrada, con amenaza concreta, grave, actual o razonablemente inminente, y con imposibilidad de obtener la información mediante medios menos intrusivos.

En buena cuenta, "objetivos de inteligencia" es una categoría demasiado amplia para una herramienta tan intrusiva. Para spyware, el estándar debería ser seguridad nacional estricta, no mera utilidad informativa.

b) Clasificación total del procedimiento

El artículo 32.2 establece que todo el proceso constituye información clasificada como secreta. Ello puede ser comprensible respecto de detalles operativos, fuentes, identidades o capacidades técnicas. Sin embargo, como desarrollamos previamente, una clasificación total dificulta el control, el acceso a remedios y la identificación de abusos.

Creemos que sí es razonable la reserva en inteligencia. Sin embargo, tratándose de spyware, la clasificación no debería impedir mecanismos de transparencia ex post, control agregado o revisión independiente. De lo contrario, el secreto protege no solo la operación legítima, sino también la posible ilegalidad. En buena cuenta, una cosa es reservar el detalle operativo; otra muy distinta es clausurar toda posibilidad de saber si el Estado usa spyware, cuántas veces lo autorizó, con qué controles y bajo qué criterios generales.

c) Ausencia de reglas específicas sobre spyware

Al igual que el Código Procesal Penal, el régimen de inteligencia no contiene reglas técnicas específicas para software intrusivo. No regula límites de acceso, minimización, destrucción verificable, auditoría técnica, participación de proveedores, infraestructura extranjera, integridad de datos, riesgos de manipulación o mecanismos de desinstalación.

Esta omisión resulta especialmente problemática porque la ley sí contiene una regla de destrucción de información innecesaria. Como desarrollamos previamente, el artículo 35 del Decreto Legislativo N.° 1141 dispone que toda información obtenida para inteligencia que sea innecesaria para el objetivo del sistema, por corresponder a derechos fundamentales y a la esfera de vida privada, debe ser destruida bajo responsabilidad. Sin embargo, para que esta regla sea efectiva frente al spyware, debe existir capacidad de verificar qué se obtuvo, qué fue usado, qué fue destruido y quién lo controló. La obligación de destruir información innecesaria es correcta, pero insuficiente si no existe trazabilidad técnica. Si nadie puede verificar la destrucción, la garantía queda en papel, pero sin posible eficiencia en la práctica.

3. SPYWARE EN EL PERÚ: NECESIDAD DE MORATORIA Y RECOMENDACIONES DE POLÍTICA PÚBLICA

3.1. Moratoria sobre la venta, transferencia y uso de tecnologías de spyware

A partir del análisis constitucional y legal realizado, así como de los límites de transparencia y el marco normativo de inteligencia desarrollado previamente, reafirmamos la posición sostenida por diversas organizaciones de sociedad civil[53], entre ellas Hiperderecho, así como por

[53] Amnistía Internacional, Joint open letter by civil society organizations and independent experts calling on states to implement an immediate moratorium on the sale, transfer and use of surveillance technology, Julio, 2021 https://www.amnesty.org/en/documents/doc10/4516/2021/en/

organismos internacionales y expertos independientes[54]: **el Perú debe establecer una moratoria sobre la venta, transferencia, adquisición y uso de tecnologías de spyware.**

Esta es una recomendación de política pública que parte de una constatación concreta: el spyware es una herramienta cualitativamente distinta a otras formas de vigilancia. No se limita a interceptar una comunicación, monitorear una ubicación o acceder a un registro específico. Por el contrario, permite comprometer el dispositivo completo de una persona y, con ello, acceder de forma encubierta a mensajes, archivos, fotografías, ubicación, contactos, metadatos, micrófono, cámara y aplicaciones de comunicación cifrada.

El software de espionaje no vigila una conducta aislada: puede capturar la vida digital entera de una persona. Por ello, resumimos a continuación las razones por las cuales consideramos que debe establecerse una moratoria.

En primer lugar, y a diferencia de la vigilancia tradicional, el spyware permite un nivel de intrusión en la vida sin precedentes ya que habilita un acceso total, encubierto y persistente al dispositivo[55]. Esto genera una afectación simultánea de múltiples derechos: privacidad, intimidad, secreto de comunicaciones, autodeterminación informativa, libertad de expresión, libertad de asociación, defensa legal y protección de fuentes

[54] Como el Relator Especial de la Organización de las Naciones Unidas (ONU) sobre la promoción y protección del derecho a la libertad de opinión y de expresión; la Alta Comisionada de las Naciones Unidas para los Derechos Humanos; el Gobierno de Costa Rica; Amnistía Internacional; Access Now; Cyber Peace Institute. Ver, entre otros, Anstis, Siena, y Jillian Sprenger. Loc. Cit; Kaldani, Tamar, y Zeev Prokopets. Loc. Cit.; Kaye, David. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. Ginebra: Naciones Unidas, Consejo de Derechos Humanos, A/HRC/41/35, 2019. https://documents.un.org/doc/undoc/gen/g19/148/76/pdf/g1914876.pdf.; Relatoría Especial para la Libertad de Expresión (RELE). Loc. Cit.; ; Cyber Peace Institute, *Renewed Call for Moratorium on Sale and Use of spyware*, Mayo, 2022; OACNUDH, Procedimientos especiales, spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech 12 de agosto de 2021

[55] Anstis, Siena, y Jillian Sprenger. Loc. Cit; Relatoría Especial para la Libertad de Expresión (RELE). Loc. Cit

periodísticas. Ello plantea un problema de proporcionalidad reforzada: no basta con preguntar si la medida puede ser útil para investigar delitos o producir inteligencia; la pregunta constitucionalmente relevante es si el Estado puede justificar una intrusión tan extensa sin vaciar de contenido los derechos fundamentales afectados.

El segundo argumento es que el spyware no afecta un solo derecho, sino un conjunto articulado de libertades y derechos fundamentales (de forma directa o indirecta como hasta aquí desarrollamos). Directamente compromete la privacidad, los datos personales y las comunicaciones; indirectamente produce efectos inhibitorios sobre la libertad de expresión, reunión, asociación, prensa y defensa de derechos humanos[56]. En efecto, una persona que sabe o sospecha que puede ser vigilada modifica su conducta: deja de conversar, evita reunirse, reduce su actividad política, limita sus investigaciones, abandona fuentes o restringe su participación pública.

Una tercera razón es que hay un uso documentado del software de espionaje contra actores clave del sistema democrático. En distintos países se ha documentado el uso de spyware contra periodistas, defensores de derechos humanos, opositores políticos, entre otros[57]. Ello contradice la narrativa usual según la cual estas herramientas se adquieren exclusivamente para combatir terrorismo, crimen organizado o amenazas extremas. La experiencia comparada demuestra que este tipo de software tiene, por tanto, un riesgo especialmente alto de desviación funcional. Una tecnología creada o vendida para combatir amenazas graves puede terminar siendo utilizada para perseguir disidencia o neutralizar investigaciones periodísticas. En buena cuenta, el problema no es solo lo que el spyware promete hacer, sino lo que en la práctica permite hacer a gobiernos con incentivos de opacidad y autoritarismo.

---

56 Kaldani, Tamar, y Zeev Prokopets. Loc. Cit; Relatoría Especial para la Libertad de Expresión (RELE). Loc. Cit

57 Anstis, Siena, y Jillian Sprenger. Loc. Cit.; Kaldani, Tamar, y Zeev Prokopets. Loc. Cit; Relatoría Especial para la Libertad de Expresión (RELE). Loc. Cit

El cuarto argumento gira en torno a la falta de mecanismos efectivos de transparencia y rendición de cuentas. Como desarrollamos hasta aquí, en el Perú, las rutas posibles de adquisición de spyware se ubican precisamente en zonas de baja visibilidad: contrataciones directas por secreto, información clasificada, inteligencia, orden interno, recursos especiales y cooperación con proveedores extranjeros. A ello se suma que la legislación permite reservar información cuando se invoca seguridad nacional, inteligencia o investigaciones en curso.

No obstante ello, la reserva no debería operar como una cláusula absoluta. El problema es que, en la práctica, el spyware combina dos capas de ocultamiento[58]: a) ocultamiento técnico, porque la persona afectada normalmente no sabe que su dispositivo fue infectado; y b) ocultamiento legal, porque el Estado puede invocar secreto, reserva, inteligencia o seguridad nacional para impedir el acceso a información sobre adquisición, uso y control. De esta manera, el software espía se ubica en una zona especialmente difícil de fiscalizar. Así, si no se sabe que existe la herramienta, no se sabe quién la compró; si no se sabe quién la compró, no se sabe quién la usó; y si no se sabe quién la usó, no hay responsabilidad posible.

La quinta razón se refiere a la inexistencia e imposibilidad de recursos judiciales y de reparación. El carácter encubierto del spyware impide que la víctima conozca oportunamente la afectación[59]. Sin notificación, no hay posibilidad real de impugnar. Sin información sobre la adquisición o el uso, no hay prueba suficiente de que se ha usado: la persona afectada debe demostrar una intrusión que fue diseñada para no ser visible y, además, enfrentar un aparato estatal que puede responder con reserva, secreto o seguridad nacional. Si no es posible impugnar, más complicado es buscar una reparación a los daños causados por su uso.

58 Relatoría Especial para la Libertad de Expresión (RELE). Loc. Cit

59 Ídem.

De acuerdo a ello, la moratoria que proponemos debe tener efectos normativos e institucionales concretos. En ese sentido, debería comprender, como mínimo:

1. **Suspensión de nuevas adquisiciones** de spyware por parte de entidades públicas, incluidas Fuerzas Armadas, Policía Nacional, componentes del SINA, ministerios, organismos adscritos, gobiernos regionales y locales.
2. **Prohibición temporal de uso operativo** de herramientas ya adquiridas.
3. **Inventario público** de toda herramienta de spyware o software intrusivo adquirido, contratado, donado, transferido o recibido mediante cooperación internacional.
4. **Informe público agregado**, que permita conocer, sin comprometer operaciones legítimas, si el Estado ha adquirido estas tecnologías, qué entidades las poseen, bajo qué marco legal, de parte de qué proveedores y con qué controles.
5. **Mecanismo de recepción de denuncias y peritaje independiente** para personas que sospechen haber sido afectadas por spyware estatal.

3.2. Garantías mínimas para habilitar la adquisición y uso de spyware en Perú

Ahora bien, una vez expuesta la necesidad de establecer, como política, una moratoria respecto del spyware, cabe analizar bajo qué supuestos podría admitirse su uso en un Estado Constitucional. A continuación, las presentamos agrupándolas según su naturaleza jurídica:

3.2.1. Garantías de transparencia y publicidad

Estas son aquellas que responden a la pregunta de si puede la sociedad saber que existe este poder y cómo se usa en términos agregados. Sostenemos que sí y no hay supuestos en los cuales la sociedad pueda no conocer que el Estado está adquiriendo una tecnología así. Estas serían:

i. Transparencia en adquisición[60]: no puede haber reserva sobre la compra de spyware, independientemente de si la realiza la PNP, las FFAA, servicios de inteligencia o con recursos especiales. El procedimiento de negociación, convocatoria y compra debe estar guiado por el principio de publicidad. El interés público en conocer la mera existencia de esta capacidad estatal no admite excepciones.

ii. Aplicar, en la medida de lo posible, procedimientos de adquisición competitivos. Esto implica minimizar al máximo las contrataciones directas y priorizar, más que el costo efectivo del recurso, su menor lesividad en derechos fundamentales.

iii. Transparencia agregada[61] sobre su uso. Es necesario publicaciones periódicas de estadísticas, como mínimo, sobre: número de solicitudes, autorizaciones, rechazos, delitos invocados, duración y entidades solicitantes.

3.2.2. Mínimos respecto de proveedores

No toda empresa (nacional o extranjera) debería poder contratar con el Estado para proveer un software de tan alto riesgo. Esta debería cumplir, como mínimo, con lo siguiente:

iv. Contar con auditorías empresariales en materia de derechos humanos.

v. El proveedor deber haber realizado un estudio de impacto en derechos fundamentales respecto de su producto[62].

vi. No contar con un historial documentado de proveer spyware a regímenes o Estados que utilizaron la herramienta para violar derechos humanos[63].

vii. Prohibición de adquirir o usar proveedores que no permitan

---

60 Transparency International. *Out of the Shadows: Promoting Transparency in the Procurement of Surveillance Technologies.* Berlín: Transparency International, 2021.

61 Access Now. *Principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones* (Principios de Necesidad y Proporcionalidad). Mayo de 2014.

62 Fionnuala Ní Aoláin. Regulación mundial del comercio de tecnología de software espía para la lucha contra el terrorismo: propuestas para un enfoque respetuoso con los derechos humanos, abril de 2023.

63 Human Rights Watch, L*ooking the Other Way: EU Failure to Prevent Surveillance Exports to Rights Violators* (Bruselas: Human Rights Watch, 2026), https://www.hrw.org/report/2026/05/12/looking-the-other-way/eu-failure-to-prevent-surveillance-exports-to-rights.

auditoría independiente ni garanticen control soberano sobre la herramienta.

viii. El producto debe incorporar mecanismo de apagado en caso de mal uso[64].

ix. La empresa debería contar con, al menos, un representante legal en el territorio nacional.

3.2.3. Legalidad y habilitación normativa explícita, taxativa y detallada

Estas abordan la problemática de que debe existir una norma lo suficientemente precisa que autorice su uso. En tanto estamos ante una limitación múltiple a derechos fundamentales con una sola actividad estatal, esta debería, como mínimo:

x. Tener un marco legal autoritativo con una norma con rango de ley estricta. Es decir, norma emitida por el Congreso para garantizar la deliberación democrática. Facultades legislativas delegadas en el Ejecutivo no deberían ser viables.

xi. Esta norma debe generar una base legal específica[65] y expresa para software intrusivo, evitando la dispersión en normas de inteligencia, crimen organizado o interceptación de comunicaciones. Para el caso peruano, su posibilidad de uso para el proceso penal y en el procedimiento especial de inteligencia, debe estar concentrado en un solo cuerpo normativo que regule expresamente capacidades, supuestos permitidos y límites técnicos.

xii. Finalidad taxativamente[66] definida.

a. En lo referido a inteligencia, solo frente a amenazas graves de seguridad nacional, concretas, inmediatas e inminentes.

b. En los procesos penales, frente a delitos extremadamente graves definidos en la norma (cuyo criterio iría más allá de la

64 Fionnuala Ní Aoláin. Loc. Cit.

65 Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos [ONU OHCHR]. *El derecho a la privacidad en la era digital: Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos*. A/HRC/51/17 (4 de agosto de 2022).

66 Access Now. Loc. Cit.

cantidad de pena, sino de la lesividad social, el bien jurídico protegido, la complejidad en su investigación, la posibilidad de graves amenazas a la vida e integridad en delitos conexos demostrables, inminentes y certeros.

xiii. Se prohíbe su uso en investigación prospectiva, protesta social, inteligencia política, delitos menores y vigilancia preventiva amplia[67].

3.2.4. Autorización judicial

Como sostuvimos previamente, el uso de spyware únicamente debería autorizarse a través de una orden judicial. Ahora, esta debería tener las siguientes características mínimas:

xiv. Autorización judicial previa, individualizada y técnicamente informada[68].

xv. La orden debe identificar: persona afectada, dispositivo, medida, alcance, duración, finalidad, capacidades habilitadas y prohibiciones expresas[69].

xvi. Motivación altamente reforzada:

a. Necesidad estricta: demostrar que ningún medio menos intrusivo puede alcanzar el mismo fin[70].

b. Proporcionalidad reforzada: el juez debe ponderar la intensidad de intrusión sobre todos los derechos afectados: no solo privacidad, sino también libertad de expresión, asociación, defensa legal, secreto profesional, fuentes periodísticas y participación política[71].

---

67 Ibidem.

68 Relator Especial de la ONU sobre la promoción y protección del derecho a la libertad de opinión y de expresión. Loc. Cit.

69 Consejo de Europa. Comité de Ministros. *Recomendación CM/Rec(2014)6 del Comité de Ministros a los Estados miembros sobre una guía de derechos humanos para los usuarios de internet.* 16 de abril de 2014.

70 Access Now. Loc. Cit.

71 Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. Loc. Cit.

3.2.5. Garantías de ejecución técnica

Ahora bien, una vez autorizada la medida a través una orden judicial, es importante abordar la cuestión de cómo se ejecuta la medida y qué está prohibido hacer durante su ejecución. Sobre ello, estos serían lo mínimos indispensables:

> xvii. Minimización y segmentación técnica: la herramienta debe limitarse estrictamente a lo autorizado, sin captura indiscriminada.
>
> xviii. Prohibición de modificar o manipular datos del dispositivo[72][73].
>
> xix. Límites específicos sobre: instalación y desinstalación del software; carpetas, aplicaciones o sensores accesibles (cámara, micrófono, giroscopio, etc).
>
> xx. Destrucción verificable de información irrelevante, especialmente datos íntimos, datos de terceros, información amparada por secreto profesional, fuentes periodísticas o defensa legal[74].

3.2.6. Registro, trazabilidad y cadena de custodia

En miras a asegurar que el control institucional y el control ciudadano posterior pueda ser viable, es necesario que se guarde registro de lo realizado. Para ello, es necesario[75] que se prevea:

> xxi. Registro técnico de cada acceso, extracción, activación o transferencia, para revisión judicial o institucional.
>
> xxii. Trazabilidad de operadores: saber quién accedió, qué datos extrajo, por cuánto tiempo y bajo qué orden[76].

---

72 Marczak, Bill, John Scott-Railton, Siddharth Prakash Rao, Claudio Guarnieri y Ron Deibert. *Operating in the Shadows: Inside the Global spyware Industry.* Toronto: Citizen Lab, Universidad de Toronto, 2017.

73 Amnistía Internacional. *Forensic Methodology Report: How to Catch Pegasus.* Londres: Amnesty International Security Lab, 2021.

74 Parlamento Europeo. *Recomendación del Parlamento Europeo, de 15 de junio de 2023, a raíz de la investigación sobre la infracción y la mala administración en la aplicación del Derecho de la Unión en relación con el uso de Pegasus y otros programas espía equivalentes.* 2022/2077(INI)

75 Amnistía Internacional. *The Pegasus Project: Law Enforcement and Forensic Analysis.* Londres: Amnesty International Security Lab, 2021.

76 Fionnuala Ní Aoláin. Loc. Cit.

xxiii. Cadena de custodia digital reforzada de la información recogida.

xxiv. Control de integridad forense[77].

3.2.7. Notificación y recurso efectivo

Es necesario que una persona que ha sido objeto de una medida tan intrusiva cuenta con los mecanismos suficientes para poder ejercer sus derechos frente a esta. Así, es indispensable que una vez usado el spyware:

xxv. Se genere una notificación posterior[78] a la persona afectada una vez desaparecido el riesgo que justificó la reserva, salvo decisión judicial motivada y temporalmente limitada.

xxvi. Sea posible un reexamen judicial de la medida.

xxvii. Se incorporen remedios efectivos:

a. Para el proceso penal, exclusión probatoria del material obtenido ilícitamente, responsabilidad penal de los agentes, reparación civil y sanciones administrativas.

b. Para el caso del procedimiento especial de inteligencia, imposibilidad de usar la información en cualquier tipo de proceso o procedimiento, conforme a ley.

3.2.8. Garantías frente a sujetos especialmente protegidos

Como hemos podido observar, quienes son víctimas de spyware suelen ser personas que juegan un rol especial en la democracia. En este sentido, deberían existir categorías de personas[79] sobre las cuales debería excluirse la posibilidad de usar esta vigilancia intrusiva:

---

77 Amnistía Internacional. *Forensic Methodology Report* (...) Loc. Cit.

78 Fionnuala Ní Aoláin. Loc. Cit.

79 Comisión Interamericana de Derechos Humanos [CIDH]. Relatoría Especial para la Libertad de Expresión. *Estándares para una internet libre, abierta e incluyente*. OEA/Ser.L/V/II. CIDH/RELE/INF.17/17 (15 de marzo de 2017).

xxviii. Prohibición absoluta respecto de periodistas, defensores de derechos humanos, abogados en ejercicio de la defensa, opositores políticos, sindicalistas, líderes sociales y personas vinculadas a protesta social.

xxix. Excepción solo bajo estándares sustancialmente más altos y con control externo independiente, no bajo el régimen ordinario, en el marco de un proceso penal por delitos no conexos a las actividades que realiza y altamente lesivos de bienes constitucionales.

3.2.9. Control independiente y auditoría

Es imperativo que el control del uso de spyware recaiga en entidades o autoridades distintas a quienes solicitan y/o ejecutan la medida. Así, se debería regular[80]:

xxx. Auditoría técnica independiente antes y después del uso

xxxi. Auditorías periódicas sobre el software de espionaje mismo.

xxxii. Control independiente ex post por órganos especializados según sus funciones

a. Para control político y cuestiones de inteligencia: el Congreso a través de su Comisión de Inteligencia

b. Para el resguardo del uso debido de los recursos relacionados: Contraloría

c. Para la defensa de la población y en labor de control de la actuación estatal: Defensoría del Pueblo

d. Materias relacionadas a protección de datos y transparencia: La Autoridad Nacional de Transparencia y Protección de Datos Personales.

80 Access Now. Loc. Cit.

CONCLUSIONES

- Cuando el Estado ejerce la vigilancia digital como una potestad pública, se difumina la frontera entre la vigilancia masiva y la dirigida (pues interceptar a un objetivo implica capturar a toda su red de contactos e interacciones), exigiendo de manera obligatoria estándares constitucionales altísimos cuando se utiliza.

- El software espía (como Pegasus) unifica de forma remota, encubierta e indetectable (mediante ataques de "cero clics") todas las herramientas de vigilancia posibles al tomar el control absoluto del smartphone o computadora, los cuales constituyen el centro de la identidad, memoria, finanzas y relaciones de un individuo.

- El usar spyware implica una afectación sistemática, plural y multidimensional de los derechos fundamentales ya que su uso restringe varios de ellos, de forma directa o indirecta. Entre los directamente afectados, podemos encontrar el derecho a la vida privada e intimidad, el derecho a la protección de datos personales, el derecho al secreto e inviolabilidad de las comunicaciones, el derecho al debido proceso (y defensa), el principio/derecho de dignidad humana. Los que se podrían afectar indirectamente son: libertad de expresión, opinión e información; el secreto profesional, la libertad de reunión y asociación, a la integridad física, psíquica y moral; y la libertad de pensamiento, conciencia y religión

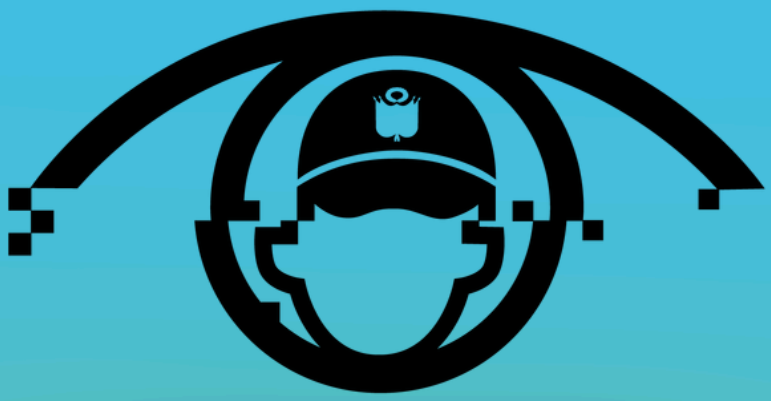
- La contratación directa no competitiva y el paraguas del "secreto" operan en la práctica como una gran compuerta hacia la opacidad absoluta; si bien la reserva puede proteger detalles estrictamente operativos, una democracia constitucional exige que la existencia misma del contrato, el monto global invertido, la entidad adquirente y las salvaguardas aplicadas permanezcan visibles.

- La clasificación de información solo es legítima si ampara actividades desarrolladas dentro del marco del Derecho. Si la actividad material de inteligencia es ilegal o abusiva, la reserva carece de sustento constitucional y debe habilitarse de inmediato el control ciudadano, parlamentario y judicial.

- En el panorama jurídico peruano actual, el uso de spyware carece de viabilidad constitucional y legal debido a dos razones normativas insalvables:
    - El Artículo 230 del Código Procesal Penal es completamente insuficiente, pues regula la interceptación de comunicaciones específicas en tránsito o la geolocalización básica, mientras que el spyware ejecuta una intrusión forense digital integral que, además, posee la capacidad de modificar, extraer o fabricar datos internamente, comprometiendo la integridad de la evidencia penal.
    - Los procedimientos especiales del SINA carecen de salvaguardas adecuadas debido a la alarmante amplitud del concepto "objetivos de inteligencia" y la falta de mecanismos técnicos independientes para auditar y verificar la destrucción obligatoria de la información innecesaria recolectada.

- Urgencia de una moratoria inmediata: Ante la severa afectación de derechos fundamentales y el riesgo inminente para la democracia, se concluye la necesidad imperativa de declarar una moratoria sobre la venta, transferencia, adquisición y uso de tecnologías de spyware en el Perú, en tanto no se cuente con un marco regulatorio compatible con los estándares internacionales.

- Garantías mínimas exigibles para habilitar su uso: verdadera transparencia; control estricto de proveedores; habilitación judicial con proporcionalidad reforzada; prohibición respecto del uso de spyware en roles democráticos; auditoría técnica externa e independiente.



HIPERDERECHO