Tendencias y prácticas de vigilancia en América Latina.

Estudios de caso de Brasil, Chile, Colombia, El Salvador, México, Perú y Paraguay



AlSur

Tendencias y prácticas de vigilancia en América Latina.

Estudios de caso de Brasil, Chile, Colombia, El Salvador, México, Perú y Paraguay

COORDINACIÓN:
Silvia Calderón, Instituto Panamericano de Derecho y Tecnología (IPANDETEC)
Ana Gaitán, Red en Defensa de los Derechos Digitales (R3D)

AUTORÍA Y REVISIÓN:
Helena Secaf - Centro de Pesquisa InternetLab
Vitor Vilanova - Centro de Pesquisa InternetLab
María Parra - Fundación Karisma
Lucia Camacho - Derechos Digitales
Laura Mantilla - Derechos Digitales
Maricarmen Sequera - TEDIC
Dilmar Villena - Hiperderecho
Ana Gaitán - Red en Defensa de los Derechos Digitales (R3D)
Silvia Calderón - Instituto Panamericano de Derecho y Tecnología (IPANDETEC)

REVISIÓN:
Camila Leite - Instituto de Defesa de Consumidores (IDEC)
Luã Cruz Instituto de Defesa de Consumidores (IDEC)

DISEÑO:
Marcelo Lazarle

ELABORADO PARA EL CONSORCIO:

CON EL FINANCIAMIENTO DE:

CHARLES STEWART MOTT FOUNDATION

JUNIO 2025

Este trabajo se distribuye con licencia Reconocimiento 4.0 Internacional (CC BY 4.0)

Esto significa que usted es libre de:

- **Compartir —** copiar y redistribuir el material en cualquier medio o formato para cualquier propósito, incluso comercialmente.
- **Adaptar —** remezclar, transformar y crear a partir del material para cualquier finalidad, incluso comercialmente.

La licenciante no puede revocar estas libertades en tanto usted siga los términos de la licencia.

Bajo los siguientes términos:

- **Atribución —** Usted debe dar crédito de manera adecuada, brindar un enlace a la licencia, e indicar si se han realizado cambios. Puede hacerlo en cualquier forma razonable, pero no de forma tal que sugiera que usted o su uso tienen el apoyo de la licenciante.
- **No hay restricciones adicionales —** No puede aplicar términos legales ni medidas tecnológicas que restrinjan legalmente a otras a hacer cualquier uso permitido por la licencia.

Acceda a una copia completa de la licencia en:
https://creativecommons.org/licenses/by/4.0/legalcode.es

AlSur

"AlSur" es un consorcio de 11 organizaciones que trabajan en la sociedad civil y en el ámbito académico en América Latina y que buscan con su trabajo conjunto fortalecer los derechos humanos en el entorno digital de la región.

ORGANIZACIONES QUE COMPONEN AL SUR

- Asociación por los Derechos Civiles (ADC) - Argentina
- Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) - Argentina
- Coding Rights - Brasil
- Derechos Digitales - Regional
- Fundación Karisma - Colombia
- Hiperderecho - Perú
- Instituto Brasileiro de Defesa do Consumidor (IDEC) - Brasil
- Instituto Panamericano de Derecho y Tecnología - Centroamérica
- InternetLab - Brasil
- Red en Defensa de los Derechos Digitales (R3D) - México
- TEDIC - Paraguay

Índice

INTRODUCCIÓN 6

CAPÍTULO UNO: ESTÁNDARES DE DERECHOS HUMANOS APLICABLES A LA VIGILANCIA DE COMUNICACIONES 9

I. **Principio de reserva de ley: Definición clara, precisa y detallada de las autoridades facultadas, el procedimiento y circunstancias en las que pueden llevarse a cabo medidas de vigilancia.** 10

II. **Principios de necesidad y proporcionalidad: Salvaguardas contra el abuso.** 12
1. Finalidad constitucionalmente válida 12
2. Idoneidad de la medida 13
3. Necesidad de la medida 13
4. Estudio de proporcionalidad en estricto sentido de la medida 13

III. **Salvaguardas** 14
1. Control judicial 15
2. Medidas de transparencia y supervisión independiente 15
3. Derecho de notificación 16

En resumen 16

CAPÍTULO DOS: NORMAS Y PROCEDIMIENTOS QUE REGULAN LA VIGILANCIA DE LAS COMUNICACIONES 17

I. **¿Quién, en qué casos y bajo qué procedimientos pueden llevarse a cabo medidas de vigilancia de comunicaciones?** 17

II. **Salvaguardas fundamentales** 20

En resumen 22

CAPÍTULO TRES: CASOS DE VIGILANCIA DE COMUNICACIONES EN LA REGIÓN SEGÚN EL TIPO DE VIGILANCIA EMPLEADA 25

I. **Intervención de comunicaciones privadas** 25
COLOMBIA 26
CHILE 28

II. **Colaboración de empresas de telecomunicaciones en el acceso a registro de datos conservados** 31
PARAGUAY 31
CHILE 32
MÉXICO 33

III. **Extracción de información** 34
MÉXICO 35
PARAGUAY 35

IV. **Spyware** 35
PARAGUAY 36
MÉXICO 37
EL SALVADOR 38

V. **Geolocalización basada en la explotación de vulnerabilidades en la infraestructura de telecomunicaciones (SS7)** 40
BRASIL 40
PERÚ 42

VI. **Ciberpatrullaje** 44
COLOMBIA 44

VII. **Vigilancia de personas a través de sistemas de lectura de matrículas de automóviles** 47
BRASIL 47
En resumen 50

CAPÍTULO CUATRO: DIAGNÓSTICO 52
I. Requisitos de procedencia material 52
II. Control judicial 53
III. Proliferación de tecnologías de vigilancia masiva 54
IV. Falta de transparencia y corrupción en la adquisición de tecnologías de vigilancia 55
CONCLUSIONES 57
RECOMENDACIONES A LOS ESTADOS 58

ÍNDICE DE TABLAS

Tabla 1. Autoridades facultadas por país para intervenir comunicaciones (con o sin orden judicial) y circunstancias y procedimientos por los cuales se pueden intervenir comunicaciones 18

Siglas

SIGLA	DEFINICIÓN
ABIN	Agencia Brasileña de Inteligencia
ADO	Acción Directa de Inconstitucionalidad por Omisión [Brasil]
ADPF	Acción de Incumplimiento de Precepto Fundamental [Brasil]
AFDD	Agrupación de Familiares de Detenidos Desaparecidos [Chile]
AFEP	Agrupación de Familiares Ejecutados Políticos [Chile]
ANEF	Agrupación Nacional de Empleados Fiscales [Chile]
Bacib	Batallones de Ciberinteligencia [Colombia]
BIPE	Brigada de Investigaciones Policiales Especiales [Chile]
CADH	Convención Americana de Derechos Humanos
Caso CAJAR	Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia
CIDH	Comisión Interamericana de Derechos Humanos
CNPP	Código Nacional de Procedimientos Penales [México]
Corte IDH	Corte Interamericana de Derechos Humanos
Córtex	Plataforma Integrada de Operaciones y Monitoreo de Seguridad Pública [Brasil]
CUT	Central Unitaria de Trabajadores [Chile]
DIGIMIN	Dirección General de Inteligencia [Perú]
DINI	Dirección Nacional de Inteligencia [Perú]
FEADLE	Fiscalía Especial para la Atención de Delitos Cometidos contra la Libertad de Expresión [México]
FECH	Federación de Estudiantes de la Universidad de Chile
FEDEUNAP	Federación de Estudiantes de la Universidad Arturo Prat [Chile]
FGN	Fiscalía General de la Nación [Colombia]
FLIP	Fundación para la Libertad de Prensa
ISP	Internet Service Provider
LGN	Ley de la Guardia Nacional [México]
MJSP	Ministerio de Justicia y Seguridad Pública [Brasil]
MP	Ministerio Público
OSIPTEL	Organismo Supervisor de Inversión Privada en Telecomunicaciones [Perú]
PDI	Policía de Investigaciones [Chile]
PGN	Procuraduría General de la Nación [Colombia]
PGR	Procuraduría General de la República [Brasil]
PNP	Policía Nacional de Peru
RdC	[Periodistas de] Rutas de Conflicto [Colombia]
RELE	Relatoría Especial para la Libertad de Expresión
SEDENA	Secretaría de la Defensa Nacional [México]
SEIDO	Subprocuraduría Especializada en Investigación de Delincuencia Organizada [México]
SEOPI	Secretaría de Operaciones Integradas del Ministerio de Justicia y Seguridad Pública [Brasil]
TEDH	Tribunal Europeo de Derechos Humanos
OACNUDH	Oficina Regional del Alto Comisionado de las Naciones Unidas para los Derechos Humanos para América Central y República Dominicana y el Caribe
OEA	Organización de los Estados Americanos
ONU	Organización de las Naciones Unidas

INTRODUCCIÓN

Tanto la Asamblea General como el Consejo de Derechos Humanos de las Naciones Unidas (en adelante, ONU) han subrayado que el derecho a la privacidad es uno de los fundamentos de las democracias y de la libre expresión personal y, como tal, desempeña un papel esencial en la protección y promoción de otros derechos, incluidos los derechos a la libertad de opinión, expresión, religión, reunión y asociación.[1]

Dada la interconexión de los derechos humanos, los efectos adversos de las violaciones a la privacidad pueden conllevar también violaciones a derechos como la igualdad ante la ley, el derecho a la vida, a la libertad y a la integridad personal, a un juicio justo y a un debido proceso, el derecho a la libertad de expresión, a la protesta y libertad de asociación, a la libertad de circulación, a disfrutar del más alto nivel posible de salud y a acceder al trabajo y a la seguridad social, entre otros.[2]

En esta línea, tanto el Alto Comisionado de las Naciones Unidas para los Derechos Humanos como la Relatoría Especial de la ONU sobre la promoción y protección del derecho a la libertad de opinión y de expresión han determinado que la vigilancia de las comunicaciones privadas tiene repercusiones en la sociedad civil y el discurso democrático.[3] El riesgo de ser un objetivo de vigilancia y el deseo de evitar ser blanco de la misma, lleva a las personas a autocensurarse. Cuando las personas se perciben vigiladas, alteran y limitan la forma en la que se expresan y comunican con las demás personas. Debido a este *"efecto amedrentador" (chilling effect)*, las tecnologías de vigilancia no sólo afectan a las personas cuyos datos se recopilan, sino a toda la sociedad, al interferir tanto directa como indirectamente en el libre intercambio y evolución de ideas.[4]

Históricamente, las actividades de inteligencia realizadas en América Latina, ya sea a través de autoridades civiles, policiales o militares, lejos de servir a los intereses generales de la sociedad, se han constituido en sí mismas como un riesgo para el respeto de la dignidad y derechos de las personas.

Actualmente, se ha documentado el uso progresivo por parte de los gobiernos de tecnologías para la vigilancia de comunicaciones con el fin de reprimir, censurar y perseguir a personas defensoras de derechos humanos, periodistas, activistas sociales y opositoras políticas.[5] Dicha vigilancia ha puesto en riesgo su vida e integridad personal y ha obstaculizado la denuncia y rendición de cuentas de actos de corrupción y violaciones de derechos humanos cometidas por autoridades públicas y personas o instituciones privadas.

---

1 Naciones Unidas. Asamblea General. (2017). Resolución A/RES/71/199 El derecho a la privacidad en la era digital. Disponible en: https://documents.un.org/doc/undoc/gen/n16/455/37/pdf/n1645537.pdf, Naciones Unidas. Asamblea General. (2018). Resolución A/RES/73/179. El derecho a la privacidad en la era digital. Disponible en: https://docs.un.org/es/A/res/73/179 y, Naciones Unidas. Asamblea General. (2017). Resolución A/HRC/RES/34/7. El derecho a la privacidad en la era digital. Disponible en: https://docs.un.org/es/A/HRC/RES/34/7

2 Huszti-Orbán, K., Ní Aoláin, F. (2020). Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?". Disponible en: https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/biometricsreport.pdf

3 Véase, por ejemplo, Asamblea General de Naciones Unidas (2016). Resolución A/HRC/32/38. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión. Disponible en: https://docs.un.org/es/a/hrc/32/38

4 Naciones Unidas. Asamblea General. (2013). Resolución A/HRC/23/40. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue. Párr. 24. Disponible en: https://docs.un.org/es/A/HRC/23/40

5 Naciones Unidas. Asamblea General. (2019). Resolución A/HRC/41/35. La vigilancia y los derechos humanos. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión. Párr. 1. Disponible en: https://docs.un.org/es/A/HRC/41/35

De igual manera, la mayoría de las medidas de vigilancia actuales implican la recolección y almacenamiento masivo e indiscriminado de información sobre las comunicaciones privadas de millones de personas, la inmensa mayoría de las cuales no se encuentran involucradas en la comisión de hechos delictivos. El acceso al contenido de nuestras comunicaciones, así como el análisis de los metadatos asociados a las mismas, como los datos de localización, otorga al Estado un alto poder invasivo y control sobre todas las personas, además de atentar contra la autonomía y participación cívica.

Adicionalmente, las tecnologías disponibles para realizar esas actividades se vuelven cada vez más sofisticadas. La proliferación de tecnologías de vigilancia masiva, como las antenas falsas, el *outsourcing* de vigilancia masiva, o las tecnologías de vigilancia focalizada altamente invasiva y elusiva como el *spyware*, es indicativo de la poca claridad y precisión sobre los métodos de vigilancia que actualmente pueden considerarse compatibles con las normas de derechos humanos.

Así, el presente informe, *Tendencias y prácticas de vigilancia en América Latina*, es particularmente relevante en el contexto en el que nos encontramos: democracias en deterioro, la proliferación de crimen organizado y el aumento del autoritarismo. Ante la masificación sin controles de tecnologías de vigilancia de las comunicaciones, es esencial presionar por un mayor escrutinio, control y regulación de dichas herramientas.

Por eso, este reporte documenta algunas de las maneras en las que se utilizan diversas tecnologías de vigilancia de manera opaca, secreta, discrecional y abusiva, por autoridades sin facultades legales y sin salvaguardas adecuadas para prevenir, mitigar o remediar dichos abusos.

Es importante precisar que, al referirnos a las tendencias y prácticas de vigilancia, se comprende en dicha categoría a toda técnica y tecnología de propiedad o uso estatal con la capacidad de interferir, limitar o incidir en el ejercicio del derecho a la privacidad, sea que su despliegue se encuentre amparado o no en el marco legal local.

Entre las técnicas y prácticas de vigilancia, las que se enfocan en las comunicaciones privadas son apenas una tipología entre una taxonomía más compleja de modalidades de la vigilancia. Por lo que, a pesar de que el informe se enfoca en las comunicaciones privadas, explora también otras modalidades y técnicas de vigilancia estatal que generan preocupación por su impacto en derechos humanos.

Por ejemplo, entre las técnicas y tecnologías de vigilancia enfocada en las comunicaciones,[6] se encuentran la interceptación de las comunicaciones a través de sus intermediarios, los proveedores de servicios de internet; la solicitud de datos y metadatos de los suscriptores de servicios de telecomunicaciones; la interceptación de las comunicaciones de manera directa y dirigida por los Estados a través, por ejemplo, del uso de software malicioso –*spyware*–; el uso de técnicas de vigilancia enfocadas en el monitoreo de redes sociales e internet –como el ciberpatrullaje–; el uso de tecnologías que interceptan señales de la infraestructura de las comunicaciones y dispositivos móviles –como stingrays o IMSI-Catchers–, entre otros.

Sin embargo, existen otras modalidades de vigilancia estatal cuyo foco no recae sobre las comunicaciones, sino en el seguimiento de las personas, como por ejemplo, el despliegue y uso de sistemas de reconocimiento facial –que exploramos en un informe de AlSur de 2021[7] y en otro más publicado en 2025[8]–; así como el despliegue y uso de sistemas de reconocimiento de patentes de vehículos; entre otros.

---

6 Distintas modalidades de vigilancia masiva enfocadas en las comunicaciones de las personas se exploran en los informes A/HRC/23/40 de abril de 2013; y el informe A/HRC/41/35 de mayo de 2019, ambos de la Relatoría Especial para la Libertad de Expresión de las Naciones Unidas.

7 Venturini, J.; Garay, V. (2021). Reconocimiento facial en América Latina. Tendencias en la implementación de una tecnología perversa. AlSur. Disponible en: https://www.alsur.lat/sites/default/files/2021-11/ALSUR_Reconocimiento_facial_en_Latam_ES.pdf

8 Será publicado próximamente.

Este reporte es resultado de la investigación sobre prácticas de vigilancia en América Latina por parte de las organizaciones de AlSur en Colombia, Chile, Perú, México, Paraguay y Brasil. La misma se realizó a través del monitoreo y documentación que cada una de las organizaciones participantes ha realizado en su respectivo país. La investigación delimitó su alcance temporal desde el año 2016 –en el que empezó a visibilizarse de manera exponencial en la región el uso de medidas de vigilancia de las comunicaciones– hasta finales de 2024.

Es importante mencionar que en muchos casos la legalidad de su utilización es cuestionable y en la mayoría de los casos existe una extendida opacidad respecto de su uso. No obstante, la recopilación también incluyó datos sobre el panorama legislativo, actuaciones del gobierno y entidades de seguridad, administrativas y judiciales.

En el *capítulo 1*, el informe recopila los estándares de derechos humanos aplicables a la vigilancia de las comunicaciones. El *capítulo 2* identifica las normas y procedimientos que regulan la vigilancia de las comunicaciones en distintos países de la región. El *capítulo 3* documenta casos emblemáticos en los que se utilizaron técnicas de vigilancia de comunicaciones en la región. Finalmente, el *capítulo 4* realiza un diagnóstico sobre las tendencias y prácticas en Latinoamérica, en aras de resaltar las deficiencias normativas, opacidad e irregularidades en la adquisición de tecnologías de la vigilancia, vigilancia ilegal e impunidad que han existido con respecto a la vigilancia de comunicaciones. El reporte cierra con la presentación de conclusiones y recomendaciones para los Estados sobre regulación en la materia.

CAPÍTULO UNO: ESTÁNDARES DE DERECHOS HUMANOS APLICABLES A LA VIGILANCIA DE COMUNICACIONES

El derecho a la privacidad y a la protección de datos personales son derechos humanos fundamentales, aunque no siempre se les reconoce como distintos y autónomos, pese a su relación e interdependencia. Se trata de derechos reconocidos en extensos instrumentos de derechos humanos tanto en el ámbito internacional[9] como en el regional.[10]

A nivel interamericano, la Corte Interamericana de Derechos Humanos (en adelante, "Corte IDH") ha definido a la vida privada como un derecho que: "abarca una serie de factores relacionados con la dignidad del individuo, incluyendo, por ejemplo, la capacidad para desarrollar la propia personalidad y aspiraciones, determinar su propia identidad y definir sus propias relaciones personales."[11]

En una interpretación más reciente del contenido de la CADH y del corpus iuris interamericano[12], la Corte IDH estableció que los estándares internacionales de protección de datos personales exigen que su procesamiento ocurra solamente con consentimiento libre e informado del titular de datos o de un marco normativo que se lo faculte dicho procesamiento.[13]

La protección que tiene toda persona bajo el derecho internacional de los derechos humanos a una vida privada y familiar sin injerencias arbitrarias, así como a la protección de sus datos personales, se extiende a sus comunicaciones digitales.[14] Así, la Corte IDH también se ha pronunciado en cuanto a la protección de la vida privada en el marco del proceso de comunicación, incluso los metadatos, recalcando que sus criterios "tienen plena aplicación en torno a actividades de inteligencia que supongan una vigilancia de [dichos metadatos]".[15]

Sin embargo, el derecho a la vida privada no es un derecho absoluto y el uso de actividades de inteligencia puede tener fines legítimos y ser un medio útil para la investigación de delitos y combatir amenazas a la seguridad nacional. Las limitaciones legítimas al derecho a la privacidad, deben estar alineadas a estándares en derechos humanos. En ese sentido, la Corte IDH determinó que "[l]as medidas tendientes a controlar las labores de inteligencia deben ser especialmente rigurosas, puesto que, dadas las condiciones de reserva bajo las que se realizan esas actividades, pueden derivar hacia la comisión de violaciones de los derechos humanos y de ilícitos penales".[16]

---

9 Declaración Universal de los Derechos Humanos (art. 12), el Pacto Internacional de Derechos Civiles y Políticos (art. 17), la Convención sobre los Derechos del Niño (art. 16), la Convención Internacional sobre la Protección de los Derechos de todos los Trabajadores Migratorios y de sus Familiares (art. 14), incluida la Observación General n.16 del Comité de Derechos Humanos de la ONU de 1988, entre otros instrumentos universales de los derechos humanos.

10 Convención Americana de Derechos Humanos (en adelante, "CADH"), Convención Interamericana sobre la Protección de los Derechos Humanos de las Personas Mayores, art. 11; art 12, c, ii.; enriquecido además por los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales de 2021, entre otros.

11 Corte IDH. Caso Artavia Murillo y otros (Fecundación in vitro) Vs. Costa Rica. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 28 de noviembre de 2012. Párr. 143.

12 Integrado, además, por los "Principios Actualizados del Comité Jurídico Interamericano sobre la Privacidad y la Protección de Datos Personales, con Anotaciones", OEA/Ser.D/XIX.20, enero de 2022.

13 Corte IDH. Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia, Sentencia de 18 de octubre de 2023, Excepciones Preliminares, Fondo, Reparaciones y Costas, párr. 573.

14 Distintos órganos de derechos humanos han adoptado una perspectiva expansiva sobre lo que entra dentro del ámbito de protección de la intimidad en el contexto digital, incluyendo: la vigilancia audiovisual (El Haski c. Bélgica [2012] TEDH 2019; (2013) 56 EHRR 31, [102]); los metadatos (Malone c. Reino Unido [1984] TEDH 10; (1985) 7 EHRR 14, [84]); y la información de geolocalización (Uzun c. Alemania [2010] TEDH 2263; (2011) 53 EHRR 24, [12]-[13]).

15 Corte IDH. Caso Escher y otros Vs. Brasil, supra, párr. 114; y, pár. 543.

16 Corte IDH. Caso Myrna Mack Chang Vs. Guatemala. Fondo, Reparaciones y Costas. Sentencia de 25 de noviembre de 2003. Serie C No. 101, párr. 284.

Así, para que las restricciones a los derechos a la privacidad y a la protección de datos personales cumplan con estándares nacionales, regionales[17],[18],[19] e internacionales[20] en la materia y prohíban medidas de vigilancia ilegales y arbitrarias, se deben cumplir con los requisitos de legalidad, finalidad legítima, idoneidad, necesidad y proporcionalidad[21], lo cual, a su vez, implica el establecimiento de salvaguardas adecuadas para prevenir, evitar y remediar el ejercicio abusivo de las mismas.

I. Principio de reserva de ley: Definición clara, precisa y detallada de las autoridades facultadas, el procedimiento y circunstancias en las que pueden llevarse a cabo medidas de vigilancia.

Según la Corte IDH, la reserva de ley o la expresión "leyes", a las que refiere la CADH como el medio habilitador para la limitación de derechos (art. 30), va más allá del principio de legalidad formal, abarcando a todos los actos normativos legítimos, enfocados en el bien común, y emanados de los órganos constitucional y democráticamente elegidos.[22]

Por su parte, la Declaración Conjunta sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión sostiene:

> Los Estados deben garantizar que la intervención, recolección y uso de información personal (...) estén claramente autorizadas por la ley a fin de proteger a la persona contra interferencias arbitrarias o abusivas en sus intereses privados. La ley deberá establecer límites respecto a la naturaleza, alcance y duración de este tipo de medidas, las razones para ordenarlas, las autoridades competentes para autorizar, ejecutar y supervisarlas y los mecanismos legales para su impugnación.[23]

---

17 Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. Disponibles en: https://necessaryandproportionate.org/es/necesarios-proporcionados

18 CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 31 de diciembre de 2013. OEA/Ser.L/V/II, párr. 165.

19 Corte IDH. Caso Myrna Mack Chang Vs. Guatemala, supra; Caso Maritza Urrutia Vs. Guatemala. Fondo, Reparaciones y Costas. Sentencia de 27 de noviembre de 2003. Serie C No. 103; Caso Huilca Tecse Vs. Perú. Fondo, Reparaciones y Costas. Sentencia de 3 de marzo de 2005. Serie C No. 121; Caso Blanco Romero y otros Vs. Venezuela. Fondo, Reparaciones y Costas. Sentencia de 28 de noviembre de 2005. Serie C No. 138; Caso Goiburú y otros Vs. Paraguay, supra; Caso La Cantuta Vs. Perú. Fondo, Reparaciones y Costas. Sentencia de 29 de noviembre de 2006. Serie C No. 162; Caso Escher y otros Vs. Brasil, supra; Caso Anzualdo Castro Vs. Perú. Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia de 22 de septiembre de 2009. Serie C No. 202; Caso Gelman Vs. Uruguay. Fondo y Reparaciones. Sentencia de 24 de febrero de 2011. Serie C No. 221; Caso González Medina y familiares Vs. República Dominicana. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 27 de febrero de 2012. Serie C No. 240; Caso Gudiel Álvarez y otros ("Diario Militar") Vs. Guatemala, supra; Caso García y familiares Vs. Guatemala, supra; Caso Hermanos Landaeta Mejías y otros Vs. Venezuela, supra; Caso Rodríguez Vera y otros (Desaparecidos del Palacio de Justicia) Vs. Colombia, supra; Caso Familia Julien Grisonas Vs. Argentina, supra; Caso Maidanik y otros Vs. Uruguay. Fondo y Reparaciones. Sentencia de 15 de noviembre de 2021. Serie C No. 444; Caso Movilla Galarcio y otros Vs. Colombia, supra, y Caso Deras García y otros Vs. Honduras. Fondo, Reparaciones y Costas. Sentencia de 25 de agosto de 2022. Serie C No. 462.

20 Naciones Unidas. Asamblea General. (2010). Resolución A/HRC/14/46. Informe de Martin Scheinin, Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo. Disponible en: https://docs.un.org/es/A/HRC/14/46; Naciones Unidas. Asamblea General. (2013). Resolución A/HRC/23/40. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue. Disponible en: https://docs.un.org/es/A/HRC/23/4; Naciones Unidas. Asamblea General. (2014). Resolución A/HRC/27/37. El derecho a la privacidad en la era digital, Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. Disponible en: https://docs.un.org/es/A/HRC/27/37y; Naciones Unidas. Asamblea General. (2020). Resolución A/RES/75/176. El derecho a la privacidad en la era digital. Disponible en: https://docs.un.org/es/A/RES/75/176

21 Corte IDH. Caso Tristán Donoso Vs. Panamá, supra, párr. 56, y Caso Fernández Prieto y Tumbeiro Vs. Argentina. Fondo y Reparaciones. Sentencia de 1 de septiembre de 2020. Serie C No. 411, párr. 105.

22 Corte IDH. Opinión Consultiva OC-6/86 del 9 de Mayo de 1986. La expresión "leyes" en el artículo 30 de la Convención Americana sobre Derechos Humanos. Disponible en: https://www.corteidh.or.cr/docs/opiniones/seriea_06_esp.pdf

23 CIDH. (2013). Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión. Disponible en: https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=926&IID=2

La Relatoría para la Libertad de Expresión (en adelante RELE) ha establecido que, en el contexto de medidas de vigilancia, la ley debe ser lo suficientemente clara en sus términos para otorgar a las ciudadanas de una indicación adecuada respecto de las condiciones y circunstancias en las que las autoridades estarán facultadas para recurrir a dichas medidas.[24] En igual sentido, ha apuntado que:

> Las *normas legales vagas o ambiguas* que otorgan facultades discrecionales muy amplias son incompatibles con la Convención Americana, porque *pueden sustentar potenciales actos de arbitrariedad que se traduzcan en la violación del derecho a la privacidad o del derecho a la libertad de pensamiento y expresión* garantizados por la Convención.[25]

En la misma línea, la Corte IDH ha señalado que la primera exigencia en el ejercicio de actividades de inteligencia se refiere justamente al *principio de reserva de ley* para la protección eficaz de los derechos y el "control adecuado del ejercicio de las competencias de los órganos" estatales.[26]

En cuanto a los controles y limitaciones a los que deben ser sometidas las actividades de inteligencia, la Corte IDH determinó más recientemente que las actividades de inteligencia deben estar reguladas con la mayor precisión posible, definiendo los métodos autorizados para recopilar información, los objetivos, las personas y actividades sujetas a vigilancia, el grado de sospecha que justifique la obtención, los plazos permitidos de estas medidas y los métodos de supervisión y control.[27]

Además, en el caso de permitirse el intercambio de información entre organismos de inteligencia, deben precisarse condiciones claras, fines legítimos, autoridades competentes y garantías para proteger especialmente los datos personales.[28]

Así mismo, es necesario que todas las actividades se formalicen mediante procesos numerados, incluyendo controles sobre el acceso a los sistemas, y que el procesamiento de datos personales cuente con registros que i. identifiquen a los responsables; ii. fines del procesamiento; iii. base legal; iv. plazos de conservación y; v. métodos utilizados, así como un historial de todas las acciones realizadas sobre esos datos.[29]

De igual forma, en términos de recopilación de datos personales, la Corte IDH prevé que las facultades de servicios de inteligencia (que generalmente son ejercidas con la falta de consentimiento del titular), deberán basarse en leyes que describan:

> a) los motivos que habilitan la existencia de archivos con datos personales por parte de los organismos de inteligencia; tales motivos, acordes con los fines propios de las actividades de inteligencia, habrán de limitar el actuar de las autoridades en esta materia; b) las clases y tipos de datos de carácter personal que las autoridades están facultadas para conservar en sus archivos, y c) los parámetros aplicables para la utilización, conservación, verificación, rectificación, eliminación o revelación de tales datos [...].[30]

---

24 Corte IDH. Caso Escher y otros vs. Brasil. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 6 de julio de 2009. Serie C No. 200.

25 CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 31 de diciembre de 2013. OEA/Ser.L/V/II.

26 Corte IDH. Opinión Consultiva OC-6/86, supra, párr. 24. Reiterado en Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia, Sentencia de 18 de octubre de 2023, Excepciones Preliminares, Fondo, Reparaciones y Costas. Párr. 529.

27 Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia, Sentencia de 18 de octubre de 2023, Excepciones Preliminares, Fondo, Reparaciones y Costas, párr. 520.

28 Ibidem, párr. 539.

29 Ibidem, párr. 540.

30 Ibídem, párr. 577.

II. Principios de necesidad y proporcionalidad: Salvaguardas contra el abuso.

Se presuponen *(i) una finalidad constitucionalmente válida* (de un interés jurídico preponderante y necesario en una sociedad democrática), *(ii) idoneidad* (adecuación de la restricción en el derecho con su finalidad), *(iii) necesidad de la medida* (el medio menos propenso a vulnerar los derechos humanos), y *(iv) su estudio de proporcionalidad en estricto sentido* (entre el grado de intervención en el derecho fundamental que supone la medida legislativa examinada frente al grado de realización del fin perseguido por ésta).

Por fin, es necesario que existan *(v) salvaguardas*, como el control judicial (previo o inmediato a medidas invasivas), transparencia y supervisión independiente (con rendición de cuentas) y el derecho de notificación (a las personas afectadas cuando la vigilancia ha sido completada).

1. Finalidad constitucionalmente válida

Aún cuando la intervención de comunicaciones y otras invasiones a la privacidad de las personas sean, en muchos casos, interferencias en la privacidad que persiguen fines legítimos como la investigación de delitos graves y protección de la seguridad nacional, también es claro que existen riesgos inherentes de abuso.

Por lo tanto, en primer lugar, las medidas de vigilancia deben identificar los fines que persiguen para después determinar si son constitucionalmente válidos.[31] Así, las leyes sólo deberían permitir la vigilancia de las comunicaciones por parte de autoridades estatales específicas para alcanzar un objetivo legítimo que corresponda a un interés jurídico preponderante y necesario en una sociedad democrática. En palabras del Consejo de Derechos Humanos, la vigilancia legal y específica de comunicaciones digitales puede ser una medida necesaria y eficaz para actividades de inteligencia por motivos de seguridad nacional, prevención de terrorismo u otros delitos. Puede ser un objetivo legitimo, en tanto que el grado de injerencia se contraponga a la necesidad y el beneficio de la medida para el objetivo y que se respecte el artículo 17 del Pacto.[32]

En la misma línea, en la referida Declaración Conjunta sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión, se sostiene que:

> Cuando se invoque la seguridad nacional como razón para vigilar la correspondencia y los datos personales, la ley debe especificar claramente los criterios que deben aplicarse para determinar los casos en los cuales este tipo de limitaciones resulta legítimo. Su aplicación deberá autorizarse únicamente cuando exista un riesgo cierto respecto de los intereses protegidos, y cuando ese daño sea superior al interés general de la sociedad en función de mantener el derecho a la privacidad y a la libre expresión del pensamiento y circulación de información.[33]

En este sentido, la Corte IDH precisa que los objetivos anteriores se revelan como "fines legítimos", en función de su correspondencia con un Estado de Derecho que siempre vele por la protección de los derechos de las personas.[34] De manera que, enunciados vagos e imprecisos no podrán justificar el actuar de los organismos de inteligencia, pues lo anterior implicaría apartarse de aquellos fines, sino es que incluso contradecirlos o anularlos.[35]

---

31 SCJN. Amparo en revisión 237/ 2014. Ponente: Arturo Zaldívar Lelo de Larrea. Aprobado por mayoría de votos. De este precedente surge la Tesis Aislada 1a. CCLXV/2016 (10a.) PRIMERA ETAPA DEL TEST DE PROPORCIONALIDAD. IDENTIFICACIÓN DE UNA FINALIDAD CONSTITUCIONALMENTE VÁLIDA. Registro 2013143

32 Naciones Unidas. Asamblea General. (2014). Resolución A/HRC/27/37. El derecho a la privacidad en la era digital. párr. 24.

33 CIDH. (2013). Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión. Disponible en: https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=926&IID=2

34 Corte IDH. Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia, Sentencia de 18 de octubre de 2023, Excepciones Preliminares, Fondo, Reparaciones y Costas. Párr. 533.

35 Ibídem, párr. 532.

2. Idoneidad de la medida

En segundo lugar, la grada de *idoneidad* determina si la medida impugnada es adecuada para alcanzar los fines perseguidos por el legislador o la autoridad.[36] Es decir, debe existir una relación entre la restricción en el derecho y el fin que persigue dicha afectación.

El examen de idoneidad supone la corroboración de un nexo causal entre la medida de la autoridad y su finalidad inmediata. La Suprema Corte de Justicia de la Nación de México ha señalado que esta conexión causal entre el medio y el fin "debe establecerse con premisas empíricas obtenidas a partir de conocimientos generales aceptados en la sociedad y conocimientos especializados de la ciencia y la técnica".[37]

3. Necesidad de la medida

La vigilancia de las comunicaciones sólo debe llevarse a cabo cuando es el único medio para alcanzar un objetivo legítimo, o bien, cuando habiendo varios medios, sea el menos propenso a vulnerar los derechos humanos. La carga de establecer esta justificación, tanto en los procesos judiciales como en los legislativos, recae en el Estado.

El segundo paso de estudio de la grada de necesidad consiste en analizar si la medida propuesta es menos lesiva. Es decir, cuando las medidas de vigilancia impliquen la recolección y almacenamiento masivo e indiscriminado de información sobre las comunicaciones privadas de, por ejemplo, millones de usuarias de telecomunicaciones y servicios financieros en línea, la inmensa mayoría de las cuáles en ningún momento se verán involucradas en la comisión de hechos delictivos, el principio de necesidad debe conducir a evaluar si existen medidas menos lesivas de los derechos de las personas que no están vinculadas a la investigación en cuestión, en aras de conseguir la finalidad perseguida.

4. Estudio de proporcionalidad en estricto sentido de la medida

Dicho análisis requiere comparar el grado de intervención o limitación de la privacidad que trae consigo la medida en cuestión, evaluada de cara al grado de realización del fin perseguido por ésta. El grado de afectación se potencializa frente al hecho de que las medidas de vigilancia tienden a implicar la recolección masiva e indiscriminada de información de millones de personas, la inmensa mayoría de los cuales nunca se verán involucrados en la investigación de hecho delictivo alguno. Usar herramientas de vigilancia de las comunicaciones para fines de prevención del delito es, por tanto, desproporcionado.[38] Asimismo, la información que se retiene para dicho fin suele ser excesiva en comparación con la amenaza que se busca combatir.

De acuerdo con la Corte IDH, una medida que interfiere con un derecho solamente puede considerarse *necesaria* si no existe una medida alternativa menos lesiva del derecho para conseguir el objetivo legítimo[39], y *proporcional*, si la afectación al derecho humano no resulta exagerada o desmedida frente a las ventajas que se obtienen mediante tal limitación.[40]

---

36 SCJN. Amparo en revisión 237/ 2014. Ponente: Arturo Zaldívar Lelo de Larrea. Aprobado por mayoría de votos. De este precedente surge la Tesis Aislada 1a. CCLXVIII/2016 (10a.) "SEGUNDA ETAPA DEL TEST DE PROPORCIONALIDAD. EXAMEN DE LA IDONEIDAD DE LA MEDIDA LEGISLATIVA". Registro: 2013152.

37 SCJN. Amparo en Revisión 163/2018 Citando a [1] Bernal Pulido, Carlos, El principio de proporcionalidad y los derechos fundamentales, 2ª ed., Madrid, CEPC, 2005, p. 727.

38 SURVEILLE. (2015). "Surveillance: Ethical Issues, Legal Limitations,and Efficiency", Disponible en: https://surveille.eui.eu/wp-content/uploads/sites/19/2015/04/D4.10-Synthesis-report-from-WP4.pdf p. 22

39 Corte IDH. (2008). Caso Kimel vs. Argentina, Sentencia de 2 de mayo de 2008, Serie C No. 177, párr. 74.

40 Ibídem, párr. 83.

La relevancia de garantías efectivas en contra del abuso de medidas de vigilancia electrónica encubierta también ha sido destacada por la Asamblea General de la Organización de las Naciones Unidas,[41] la Relatoría Especial de la ONU para el Derecho a la Libertad de Expresión y Opinión,[42] la Oficina del Alto Comisionado para los Derechos Humanos de la ONU,[43] la RELE[44], así como por organizaciones de la sociedad civil y expertos que han recogido las mejores prácticas derivadas de la jurisprudencia y doctrina comparada y han elaborado los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones.[45]

III. Salvaguardas

Dentro de las opciones de salvaguarda adicionales están (i) el control judicial, (ii) la transparencia y supervisión independiente y, (iii) la notificación a las personas afectadas por las medidas de vigilancia estatal.

1. Control judicial

Una de las salvaguardas fundamentales para inhibir los riesgos de abuso de las medidas de vigilancia encubierta es el control judicial. La relevancia fundamental del control judicial, previo o inmediato, ha sido resaltado por la RELE:

> Las decisiones de realizar tareas de vigilancia que invadan la privacidad de las personas *deben ser autorizadas por autoridades judiciales independientes*, que deben dar cuenta de las razones por las cuales la medida es idónea para alcanzar los fines que persigue en el caso concreto; de si es lo suficientemente restringida para no afectar el derecho involucrado más de lo necesario; y de si resulta proporcional respecto del interés que se quiere promover.[46]

En el mismo sentido, la Corte IDH ha establecido que se hace imprescindible que sean autoridades judiciales las encargadas de autorizar "medidas invasivas de recopilación de información", es decir, los métodos de obtención de información como la escucha y grabación electrónica, incluida la audiovisual, así como la pretensión de los organismos de inteligencia de requerir información referida a datos personales a empresas de telecomunicaciones, para lo cual se debe requerir de autorización judicial.[47]

La Corte IDH también reconoce que el derecho a la privacidad exige garantías específicas en torno al uso de nuevas tecnologías cuando se trata de actividades de inteligencia. Por ello, es indispensable contar con autorización judicial previa para aplicar métodos de vigilancia dirigidos a personas específicas, especialmente si implica acceder a bases de datos y sistemas de información privados que contengan datos personales, rastrear usuarios en línea o localizar dispositivos electrónicos.[48]

---

41 Naciones Unidas. Asamblea General. (2013). Resolución A/RES/68/167 sobre el derecho a la privacidad en la era digital. Disponible en: https://docs.un.org/es/A/RES/68/167

42

43 Naciones Unidas. Asamblea General. (2014). Resolución A/HRC/27/37. El derecho a la privacidad en la era digital, Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. Párr. 37. Disponible en: https://docs.un.org/es/A/HRC/27/37: "El artículo 17, párrafo 2, del Pacto Internacional de Derechos Civiles y Políticos establece que toda persona tiene derecho a la protección de la ley en contra de interferencias o ataques ilegales o arbitrarios (...) Salvaguardas internas, sin monitoreo independiente externo, han demostrado ser particularmente inefectivas contra métodos de vigilancia ilegales o arbitrarios. Mientras estas salvaguardas pueden tomar una variedad de formas, el involucramiento de todos los niveles de gobierno en la supervisión de programas de vigilancia, al mismo tiempo que una supervisión por parte de una agencia civil independiente, es esencial para asegurar una efectiva protección de la ley." (traducción propia)

44 CIDH. (2013). Relatoría Especial para la Libertad de Expresión, Libertad de Expresión e Internet, 31 de diciembre de 2013, OEA/Ser.L/V/II.

45 Ver: Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. Disponible en: https://es.necessaryandproportionate.org/text

46 CIDH. Relatoría Especial para la Libertad de Expresión, Libertad de Expresión e Internet. (2013). OEA/Ser.L/V/II, párr. 165.

47 Corte IDH. (2023). Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia, Sentencia de 18 de octubre de 2023, Excepciones Preliminares, Fondo, Reparaciones y Costas, párrs. 542, 547 y 551.

48 Ibídem, párr. 553.

De igual forma, refuerza la noción de protección especial que requiere la información obtenida y clasificada como "datos sensibles", que abarca aquellos que afectan aspectos más íntimos de las personas que puede revelar aspectos como salud, orientación sexual, creencias religiosas, filosóficas, políticas o morales, afiliaciones, datos genéticos, datos biométricos, financieros, o relacionados con menores de edad y geolocalización personal. Estos datos permiten elaborar perfiles detallados y, por su impacto y potencial para discriminar en contra de su titular, requieren una protección reforzada.[49]

Igualmente, se han reconocido otras salvaguardas indispensables para inhibir los riesgos inherentes de abuso de las medidas de vigilancia, como lo son las medidas de transparencia y la supervisión independiente o el derecho de notificación al afectado.

2. Medidas de transparencia y supervisión independiente

La RELE ha señalado que "los Estados deben establecer mecanismos de supervisión independientes sobre las autoridades encargadas de realizar las tareas de vigilancia"[50].

En igual sentido, la Relatoría Especial sobre el Derecho a la Libertad de Opinión y Expresión de la ONU ha recomendado a los Estados establecer o mantener "mecanismos nacionales de supervisión independiente y efectivos capaces de asegurar la transparencia, cuando proceda, y la rendición de cuentas por las actividades de vigilancia de las comunicaciones y la interceptación y recopilación de datos personales que realice el Estado".[51] También, ha sostenido que los Estados deben transparentar las solicitudes de intervención o acceso a las comunicaciones de las personas, su propósito e investigación a la que ésta se vincula, así como transparentar el marco legal que legitima dicha vigilancia, y los procedimientos que se aplican para dicha tarea.[52]

De igual forma, la Corte IDH ha indicado que es esencial que el marco legal contemple la existencia de un órgano civil independiente del Poder Ejecutivo y de los propios servicios de inteligencia. Esta entidad, que puede ser de naturaleza parlamentaria, administrativa o judicial, y debe contar con conocimientos técnicos adecuados y disponer de las facultades necesarias para ejercer sus funciones, incluyendo acceso total a la información necesaria para cumplir su función.[53]

3. Derecho de notificación

Otra de las salvaguardas fundamentales para proteger el derecho a la vida privada, es la obligación de parte de la autoridad de notificar a una persona que su privacidad o datos personales fueron interferidos mediante una medida de vigilancia encubierta. Si bien dicha notificación puede no llevarse a cabo de manera previa o inmediata, en tanto se podría frustrar el éxito de una investigación, sí debe ocurrir cuando ya no esté en riesgo una investigación, no exista riesgo de fuga, de destrucción de evidencia o el conocimiento pueda generar un riesgo inminente de peligro a la vida o integridad personal de alguna persona.

Este derecho de notificación a las personas afectadas por medidas de vigilancia ha sido reconocido, por ejemplo, por el Relator Especial sobre el derecho a la libertad de opinión y expresión de la ONU que sostuvo que "en cualquier caso, una vez que la vigilancia ha sido completada y se cuenta con la posibilidad de buscar la reparación que proceda respecto del uso de medidas de vigilancia de las comunicaciones".[54]

---

49 Ibídem, párr. 554.

50 CIDH. Relatoría Especial para la Libertad de Expresión, Libertad de Expresión e Internet. (2013). OEA/Ser.L/V/II, párr. 170

51 Naciones Unidas. Asamblea General. (2014). Resolución A/RES/68/167 sobre el derecho a la privacidad en la era digital. Disponible en: https://docs.un.org/es/A/RES/68/167

52 Naciones Unidas. Asamblea General. (2013). Resolución A/HRC/23/40. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue. Disponible en: https://docs.un.org/es/A/HRC/23/40

53 Corte IDH. Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia, Sentencia de 18 de octubre de 2023, Excepciones Preliminares, Fondo, Reparaciones y Costas. Párr. 564.

54 Ídem.

El derecho de notificación ha sido reconocido, además, por el Tribunal Europeo de Derechos Humanos (en adelante, TEDH), el cual determinó en el Caso Ekimdziev vs. Bulgaria que una vez que la vigilancia ha cesado y ha transcurrido el tiempo estrictamente necesario para que el propósito legítimo de la vigilancia no sea puesto en riesgo, la notificación al afectado debe llevarse a cabo sin dilación.[55]

En resumen

El derecho a la privacidad y a la protección de datos personales son derechos fundamentales reconocidos por tratados e instrumentos internacionales en materia de derechos humanos. Estos derechos se extienden al ámbito de las comunicaciones digitales, incluyendo los metadatos o datos de tráfico de las comunicaciones.

En consecuencia, para que las actividades de inteligencia sean legítimas en un Estado democrático y compatibles con los derechos humanos, las restricciones a nuestros derechos (privacidad, protección de datos personales, entre otros) deben:

- Estar previstas en una ley que sea particularmente precisa, clara y detallada de las autoridades legítimamente facultadas, describiendo el procedimiento y circunstancias en las que se pueden llevar a cabo medidas de vigilancia de las comunicaciones (principio de legalidad). Las Leyes vagas o ambiguas son incompatibles con los derechos humanos, pues pueden ser utilizadas de manera discrecional arbitraria y abusiva;
- Prever una finalidad legítima;
- Guardar una relación de causalidad con la finalidad legítima (principio de idoneidad); es decir, se requiere que la restricción de nuestra privacidad y protección de datos personales guarde una conexión con la salvaguarda de la seguridad pública o nacional;
- No existir medidas más efectivas o menos lesivas a los derechos (principio de necesidad);
- Ni ser mayor el grado de afectación a nuestros derechos que el de realización de la medida (principio de proporcionalidad).

En este sentido, la vigilancia masiva e indiscriminada de las comunicaciones es particularmente problemática, ya que afecta a personas que no están involucradas en la comisión de delitos.

Además, deben establecerse salvaguardas adecuadas para prevenir, evitar y remediar los abusos, como lo son:

- Un control judicial previo, para garantizar que las medidas de vigilancia sean autorizadas por jueces independientes que sirvan como contrapeso en el análisis acerca de si las medidas cumplieron con los principios de legalidad, necesidad y proporcionalidad.
- Transparencia y supervisión independiente, para asegurar una debida rendición de cuentas ante los posibles abusos en la adquisición y uso de medidas de vigilancia; y,
- El derecho de notificación de las personas afectadas, para asegurar el derecho de acceso a la justicia, debido proceso y recurso efectivo de las personas para impugnar medidas de vigilancia impuestas en su contra.

55 TEDH. (2007). Caso de la Asociación para la Integración Europea y los Derechos Humanos y Ekimdzhiev vs. Bulgaria, Aplicación No. 62540/00.

CAPÍTULO DOS: NORMAS Y PROCEDIMIENTOS QUE REGULAN LA VIGILANCIA DE LAS COMUNICACIONES

Los países objeto de esta investigación –Brasil,[56] México,[57] Colombia,[58] Chile,[59] Paraguay,[60] Perú[61] y El Salvador[62]– consagran a nivel constitucional la inviolabilidad de las comunicaciones, la protección de la vida privada y de los datos personales.

Ahora, se abordarán las normas y procedimientos que regulan la vigilancia de las comunicaciones en los países objetos de la investigación, enfocando la atención en:

- Autoridades facultadas en cada país para la intervención de comunicaciones privadas (con o sin orden judicial),
- Circunstancias y procedimientos por los que pueden intervenir comunicaciones y,
- Salvaguardas fundamentales para la prevención de abusos, arbitrariedades y discrecionalidad por las medidas de vigilancia.

I. ¿Quién, en qué casos y bajo qué procedimientos pueden llevarse a cabo medidas de vigilancia de comunicaciones?

Las autoridades que pretendan obtener autorización judicial, previa o posterior, para intervenir comunicaciones privadas deberán fundamentar y motivar debidamente sus solicitudes, especificando con precisión y claridad las circunstancias y procedimientos aplicados en cada medida. Como veremos, la motivación de la medida debe satisfacer criterios de necesidad, proporcionalidad, y en ocasiones, estándares probatorios de causa probable.

---

56 La Constitución Federal de Brasil garantiza estos derechos en el artículo 5, inciso XII, que protege la inviolabilidad de las comunicaciones y de la correspondencia, y en el inciso LXXIX, que reconoce la protección de datos como derecho fundamental.

57 El artículo 16 de la Constitución Política de los Estados Unidos Mexicanos reconoce el derecho a la vida privada al establecer que "nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento [...]". Además, el párrafo segundo del artículo 16 constitucional reconoce el derecho a la protección de datos personales al reconocer que "toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley [...]". Por su parte, los párrafos decimosegundo y decimotercero del artículo 16 constitucional reconocen el derecho a la inviolabilidad de las comunicaciones privadas.

58 El artículo 15 de la Constitución Política de la República de Colombia establece que ninguna injerencia en la vida privada de las personas se hará sin una ley que determine las condiciones para hacerlo y sin control judicial. De igual forma, el artículo 250 limita las autoridades y tiempos en los que debe ocurrir el proceso legal para la interceptación de comunicaciones.

59 El artículo 19 de la Constitución Política de Chile, modificada en 2024, prevé en su numeral 4to la protección de la vida privada y los datos personales.

60 El artículo 36 de la Constitución de la República de Paraguay garantiza la inviolabilidad de los documentos y comunicaciones privadas. En tal sentido, los registros documentales (cualquiera sea su formato), la correspondencia, los escritos y las comunicaciones de cualquier naturaleza no podrán ser examinados, reproducidos, interceptados o secuestrados, salvo por orden judicial para los casos específicamente previstos en la ley, y cuando ello sea indispensable para el esclarecimiento de los asuntos de competencia de las autoridades pertinentes.

61 El artículo 10 de la Constitución Política del Perú garantiza la inviolabilidad de las comunicaciones y documentos privados. Las comunicaciones, telecomunicaciones o sus instrumentos sólo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez, con las garantías previstas en la ley.

62 El artículo 24 de la Constitución de la República de El Salvador reconoce que la correspondencia de toda clase es inviolable. Además, prohíbe la interferencia y la intervención de las comunicaciones telefónicas.

Tabla 1. Autoridades facultadas por país para intervenir comunicaciones (con o sin orden judicial) y circunstancias y procedimientos por los cuales se pueden intervenir comunicaciones

PAÍS	AUTORIDADES FACULTADAS	CIRCUNSTANCIAS Y PROCEDIMIENTOS POR LOS CUALES SE PUEDEN INTERVENIR EN LAS COMUNICACIONES
Brasil	• La Agencia Brasileña de Inteligencia (en adelante, ABIN) es la principal entidad estatal autorizada para planificar, ejecutar, supervisar y controlar actividades de vigilancia con fines de inteligencia. La ABIN no tiene prerrogativa para realizar interceptaciones sin autorización judicial; sin embargo, puede acceder a información obtenida por otros órganos del Sistema Brasileiro de Inteligência (Sisbin)[63] a través de mecanismos de cooperación establecidos en la legislación vigente. • Sobre los datos de registro, sólo las autoridades policiales y el Ministerio Público (en adelante, MP) pueden solicitarlos sin orden judicial.[64]	• La Ley de Interceptación Telefónica permite la violación del secreto y la interceptación de las comunicaciones cuando haya indicios razonables de autoría o participación en un delito punible con penas de prisión;[65] • Además, el Código de Procedimiento Penal exige una motivación e indicación de elementos concretos para justificar ''la ruptura del secreto'';[66] y, • La Ley de Interceptación Telefónica prohíbe la vigilancia por tiempo indeterminado. La autorización judicial debe estar motivada, con un plazo máximo de 15 días. Este plazo puede ser renovado si es justificado.[67]
Chile	• El Ministerio Público, con la autorización previa de un juzgado de garantía que evalúa la idoneidad, necesidad y proporcionalidad de la medida.[68] • Direcciones de organismos de inteligencia con autorización judicial previa.[69]	La interceptación de las comunicaciones,[70] que se entienden como aquéllas que "simulan sistemas de transmisión de telecomunicaciones"[71] y el acceso remoto a equipos informáticos[72] deben cumplir con los siguientes requisitos de procedencia: • Deben existir "fundadas sospechas", basadas en hechos determinados de que una persona ha cometido/participado en la preparación/comisión de un delito.[73] • Deben consignarse circunstancias fácticas y jurídicas que refieran delitos puntuales y personas determinadas; y, • Debe determinarse como "estrictamente indispensable", cuando no exista otra medida investigativa para lograr el fin perseguido por las autoridades.[74]

63 La ABIN forma parte del Sisbin, que integran diversos órganos de la administración pública federal responsables de producir información relevante para las actividades de inteligencia. La operación del Sisbin está regulada por la Ley nº 9.883/99 y el Decreto nº 11.693/23.

64 Según lo previsto en normas específicas: la Ley de Organizaciones Criminales (Ley n.º 12.850/2013), la Ley de Delitos de Blanqueo de Capitales (Ley n.º 9.613/1998) y el Código de Procedimiento Penal (art. 13-A), que limita esta posibilidad a las investigaciones de delitos como el secuestro, la trata de personas, la extorsión y el envío irregular de niños o adolescentes al extranjero.

65 Ley de Interceptación Telefónica, Ley nº 9.296/1996, artículo 2, 1.

66 Código de Procedimiento Penal, Artículo 13-B.

67 Ley de Interceptación Telefónica, Artículo 8-A.

68 Código Penal Procesal, Artículo 222.

69 Ley 19974 sobre el sistema de inteligencia del estado y crea la agencia nacional de inteligencia, artículos 24 y 25.

70 Duración de la orden: Para la interceptación de comunicaciones, un plazo no mayor a 60 días, prorrogable por períodos de igual.

71 Duración de la orden: 30 días, prorrogables por períodos de hasta igual duración. Para el caso de medidas que "simulen sistemas de transmisión de telecomunicaciones", se incluyen medidas técnicas para preservar la integridad de los contenidos y de seguridad, para evitar acceso no autorizado, así como un plazo para su destrucción.

72 Duración de la orden: un plazo máximo de 30 días, prorrogables por períodos de igual duración con un máximo de 60 días.

73 Código Penal Procesal, Artículo 222.

74 Ley 19974 sobre el sistema de inteligencia del estado y crea la agencia nacional de inteligencia, artículos 24 y 25.

PAÍS	AUTORIDADES FACULTADAS	CIRCUNSTANCIAS Y PROCEDIMIENTOS POR LOS CUALES SE PUEDEN INTERVENIR EN LAS COMUNICACIONES
Colombia	• La Fiscalía General de la Nación;[75] • Autoridades de Policía Judicial;[76] • Fuerzas Militares y la Policía Nacional;[77] y, • Dirección Nacional de Inteligencia.	• Para investigar delitos y acusar a los presuntos infractores ante juzgados y tribunales competentes; • Para desarrollar actividades de inteligencia y contrainteligencia, en donde las Fuerzas Militares y la Policía Nacional son los únicos autorizados ; y, • La Fiscalía puede ordenar a la policía judicial la retención, aprehensión o recuperación de información y que ésta sea analizada por expertos en informática forense, esto con el fin de que sirva como evidencia.[78]
El Salvador	El Fiscal General de la República y el Director del Centro de Intervención son las autoridades facultadas para solicitar la intervención de las telecomunicaciones, directamente o a través de algún delegado designado por éstos, que pertenezcan al Centro, y que reúnan los mismos requisitos exigidos por esta ley para ser Director.[79]	• Para la investigación, debe existir un procedimiento de investigación de un hecho delictivo; y, • Dentro de los elementos del juicio, las investigaciones deben señalar la existencia de indicios racionales de que se ha cometido, se está cometiendo o está por cometerse un hecho delictivo establecidos en la Ley.[80]
México	• La Guardia Nacional, facultada por la Ley de la Guardia Nacional (en adelante, LGN); • La Fiscalía General de la República, facultada por el Código Nacional de Procedimientos Penales (en adelante, CNPP); y, • Las Fiscalías de las 32 entidades federativas, facultadas por el CNPP. Sin embargo, una reforma a la Ley de la Guardia Nacional –presentada en junio de 2025– propone facultar a la Secretaría de la Defensa Nacional (SEDENA) para procesar y usar información para actividades de inteligencia por motivos de seguridad nacional.	• La LGN establece un estándar de necesidad para las medidas de vigilancia de comunicaciones, constatando la existencia de indicios suficientes que acrediten que se está organizando la comisión de delitos.[81] • El artículo 16 constitucional requiere que las autoridades que pretendan solicitar a la autoridad judicial federal la autorización para llevar a cabo una intervención de comunicaciones privadas deben fundamentar y motivar sus solicitudes. • Cuando el titular del Ministerio Público "considere necesaria" la intervención dentro de una carpeta de investigación por la comisión de un delito.[82] • La Ley de Seguridad Nacional establece el estándar de necesidad, requiriendo el cumplimiento del requisito de inminencia de las amenazas a la seguridad nacional descritas en la ley.[83]
Paraguay	La Fiscalía y Policía Nacional, a través de una orden judicial y el debido proceso, pueden realizar la intercepción de las comunicaciones.[84]	La intervención de comunicaciones será excepcional.[85]

75 Constitución Política - Artículo 250. Ley 906 de 2004 (Modificado por el art. 52 Ley 1453-2011) Decreto 1704-2012 Artículo 235.

76 En cuanto al artículo 235 de la Ley 906 de 2004, este señala que corresponde a las autoridades competentes la operación técnica de la interceptación, pero no determina explícitamente cuáles son esas autoridades competentes. Sin embargo, la sentencia C-594/14 de la Corte Constitucional indica que, el art. 46 de la Ley 938-2004 "señala que dicha competencia recae en las autoridades de policía judicial".

77 Ley 1621-2013 - Artículo 3.

78 Ley 906 de 2004 (Modificado por el art. 53 Ley 1453-2011) Artículo 236.

79 Ley Especial para la Intervención de las Telecomunicaciones, con sus reformas. Decreto N.º 552.- Artículo 7.

80 Ibídem, artículo 6.

81 Ley de Guardia Nacional, artículos 100 y 103.

82 Código Nacional de Procedimientos Penales, Artículo 291.

83 Ley de Seguridad Nacional, artículos 5, 33 y 35.

84 Código Procesal Penal, artículo 198, 199, 200 y 228. Duración de la orden: 6 meses, prorrogables una vez por la misma duración.

85 Código Procesal Penal - Artículo 200.

PAÍS	AUTORIDADES FACULTADAS	CIRCUNSTANCIAS Y PROCEDIMIENTOS POR LOS CUALES SE PUEDEN INTERVENIR EN LAS COMUNICACIONES
Perú	• La Policía Nacional de Perú (en adelante, PNP) puede intervenir, sin necesidad de orden judicial, cuando se trate únicamente de acceso a metadatos de geolocalización.[86] • El Ministerio Público debe contar con orden judicial y con garantías legales,[87] actuando bajo supervisión judicial. • Organismo Supervisor de Inversión Privada en Telecomunicaciones (en adelante, OSIPTEL).[88]	• La PNP puede solicitar datos de geolocalización cuando se trate de delitos en flagrancia delictiva;[89] • El MP puede interceptar comunicaciones privadas y documentos en casos de delitos graves (corrupción, terrorismo, secuestro, lavado de dinero, entre otros);[90] y, • OSIPTEL puede solicitar a las operadoras móviles el acceso en tiempo real a datos técnicos y de geolocalización del dispositivo, para verificar la calidad del servicio de Internet móvil.[91]

Fuente: Elaboración propia con información aportada por organizaciones de AlSur.

II. Salvaguardas fundamentales

A continuación se presenta información respecto a las salvaguardas identificadas por país. Estas garantías son fundamentales para la prevención de abusos, arbitrariedades y discrecionalidad por parte de las autoridades.

En el caso de **Brasil,** se requiere de una autorización judicial para obtener metadatos, así como datos de geolocalización de las personas[92]. La ley contempla la acción de habeas data, que permite a las ciudadanas acceder a información sobre sí mismas en registros oficiales o solicitar su corrección;[93]. Asimismo, es posible interponer acciones civiles o penales contra abusos o ilegalidades cometidos en la ejecución de medidas de vigilancia. De manera excepcional, si el tribunal ante el cual se eleva la orden de vigilancia no se pronuncia en el plazo de 12 horas, el Ministerio Público o un agente de policía pueden solicitar los datos de geolocalización y metadatos directamente a las empresas de telecomunicaciones y telemática.[94]

En **Chile,** se exceptúa de las medidas de interceptación a las comunicaciones entre Abogado-Imputado y ordena a los proveedores de servicios de internet la destrucción de los datos de sus suscriptores cuando transcurra el plazo máximo de almacenamiento de dicha información.[95] También, se prevé la notificación de la medida de interceptación a la persona afectada una vez ésta haya sido ejecutada.[96]

En **Colombia,** ninguna injerencia en la vida privada de las personas se hará sin una ley que determine las condiciones para hacerlo y sin control judicial.[97] Se limita las autoridades y tiempos en los que debe ocurrir el proceso legal para la interceptación de comunicaciones.[98] Las actividades de inteligencia estarán limitadas por el "respeto de los derechos humanos y [el] cumplimiento estricto de la Constitución, la Ley y el Derecho Internacional Humanitario y el Derecho Internacional de los Derechos Humanos".[99]

---

86 Decreto Legislativo N.º 1182 – Artículo 4.3

87 Constitución Política del Perú Artículo 2.10, Ley N.º 27697 Artículo 1 y 2, Código Procesal Penal (Decreto Legislativo N.º 957) Artículo 230.

88 Resolución OSIPTEL N.º 137-2021-CD - Artículo 4.

89 Decreto Legislativo N.º 1182 – Artículo. 4.3

90 Ley N.º 27697 – Artículo 1 y 2

91 Resolución OSIPTEL N.º 137-2021-CD - Artículo 4.

92 De acuerdo con el artículo 10, § 1 del Marco Civil da Internet (Ley N ° 12.965/2014) y el artículo 13-B del Código de Procedimiento Penal.

93 Constitución Federal de la República Federativa de Brasil, artículo 5º, inciso LXXII.

94 Artículo 13-B, §4 del CPP.

95 Código Procesal Penal, artículo 222.

96 Ibídem, artículo 224.

97 Constitución Política de la República de Colombia, artículo 15.

98 Ibídem, artículo 250.

99 Ley 1621 de 2013, artículo 4.

Asimismo, y de manera excepcional, las comunicaciones entre el imputado y su abogado podrán ser interceptadas mediante autorización judicial fundada que indique hechos concretos que vinculen al abogado con el delito investigado.[100]

En **El Salvador** se podrán intervenir telecomunicaciones de manera temporal y excepcional mediante autorización judicial.[101] De manera excepcional, la resolución judicial admitirá recurso de apelación por parte del fiscal, justificando por qué causa agravio. El Juez deberá remitir los autos sin trámite ante la Cámara competente. La Cámara deberá resolver el recurso con la sola vista de los autos, en el plazo más breve posible, el cual no excederá de 24 horas contadas a partir de su recepción.[102]

En **México**[103], el artículo 16 Constitucional establece, en primer lugar, la necesidad de contar con autorización judicial federal para llevar a cabo la intervención de comunicaciones privadas,[104] requisito que reproduce también el CNPP para el acceso a datos de geolocalización en tiempo real y el acceso a datos conservados.[105] En segundo lugar, se prohíbe la intervención de comunicaciones en las materias electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor.

Existen diversas excepciones por las cuales la Fiscalía podría ordenar el acceso a datos de geolocalización o datos conservados por empresas de telecomunicaciones sin autorización judicial previa cuando esté en peligro la integridad física o la vida de una persona, o se encuentre en riesgo el objeto del delito, así como en hechos relacionados con la privación ilegal de la libertad, secuestro, extorsión o delincuencia organizada.[106] Sin embargo, existe la obligación de informar al juez de control dentro de las 48 horas siguientes a que se haya realizado el requerimiento, para efectos de que la autoridad judicial ratifique total o parcialmente la medida o revoque la misma.[107] Y en el caso de los datos de localización geográfica conservados por instituciones de crédito, las Disposiciones Administrativas que disponen la conservación y entrega de dichos datos no exigen control judicial alguno.[108]

En **Paraguay**, la intervención de las comunicaciones requiere una resolución fundada del juez;[109] y se prevé la inviolabilidad del secreto de la correspondencia realizada por los servicios de telecomunicaciones y del patrimonio documental, salvo cuando medie orden judicial.[110] De manera excepcional, se otorga tanto al juez como al Ministerio Público la facultad de requerir informes a personas o entidades públicas o privadas.[111] Dichos informes pueden solicitarse de manera verbal o escrita, incluyendo detalles sobre el procedimiento, el nombre del imputado, el lugar de entrega del informe, el plazo para su presentación y las consecuencias por incumplimiento. Por lo que, facilita el acceso a datos conservados por empresas de telecomunicaciones sin control judicial.

---

100 Código Procesal Penal, artículo 222.

101 Constitución Política de la República de El Salvador artículo 24, y Ley Especial para la Intervención de las Telecomunicaciones, con sus reformas. Decreto N.° 552.- artículo 8.

102 Ley Especial para la Intervención de las Telecomunicaciones, con sus reformas. Decreto N.° 552.- artículo 11.

103 Cabe precisar que para junio de 2025, fecha final de redacción del presente informe, se encuentran en proceso de aprobación diversas leyes en México que buscan tanto reformar el mecanismo de excepción –para ampliar los supuestos en los que puede eludirse la autorización judicial– como establecer que las autoridades de inteligencia (incluyendo al Ejército) podrán solicitar, sin ninguna salvaguarda, acceso de manera irrestricta y directa a cualquier registro público o privado, así como a una Plataforma Única de Identidad que contendrá la identificación biométrica de todas las personas como obligación para acceder a cualquier tipo de servicio.

104 Constitución Política de los Estados Unidos Mexicanos, Artículo 16.

105 Ley de la Guardia Nacional Artículo 9, fracción XXVI, y del Código Nacional de Procedimientos Penales.

106 Código Nacional de Procedimientos Penales, artículo 303.

107 Idem, artículo 303.

108 Secretaría de Hacienda y Crédito Público, Disposiciones de carácter general a que se refiere el artículo 115 de la Ley de Instituciones de Crédito.

109 Código Procesal Penal, Artículo 200.

110 Ley N° 642/95 de Telecomunicaciones, artículo 89.

111 Código Procesal Penal, artículo 228.

En **Perú** solo se pueden intervenir las comunicaciones con orden judicial motivada. La autorización judicial debe ser fundamentada, precisada en tipo de comunicación, limitada en el tiempo y la información no relacionada debe mantenerse confidencial.[112] Además, se permite la intervención de comunicaciones privadas solo en casos de delitos graves (corrupción, terrorismo, lavado de activos, etc.).[113] Finalizada la intervención, se debe notificar al afectado, quien puede impugnar judicialmente.[114] Además, procede el hábeas corpus ante interceptaciones indebidas que afecten la libertad personal[115] y el hábeas data ante un tratamiento indebido de datos personales o violación a la privacidad.[116]

De manera excepcional, y para el caso de los datos referidos a la geolocalización, la Policía podrá acceder a esta información sin necesidad de una orden judicial previa para cierto tipo de delitos. Este acceso luego debe ser convalidado a nivel judicial. En esta línea, las empresas operadoras de telecomunicaciones deben almacenar datos referidos a la geolocalización por un período mínimo de un (1) año, pudiendo ampliarse esta obligación hasta dos (2) años adicionales.[117]

En resumen

SOBRE LAS AUTORIDADES FACULTADAS, CIRCUNSTANCIAS Y PROCEDIMIENTOS PARA INTERVENIR COMUNICACIONES

A pesar de que la mayoría de los marcos legales regionales prevén requisitos generales de fundamentación y motivación, la claridad y precisión de las circunstancias y procedimientos para llevar a cabo medidas de vigilancia es variable dentro del marco jurídico regional.

Por ejemplo, en **Brasil** se requiere para la intervención de las comunicaciones privadas de *"indicios razonables"* de la comisión de un delito, basada en elementos concretos y con un plazo de tiempo determinado; en **Chile** de *"fundadas sospechas"*, basadas en circunstancias fácticas y jurídicas que refieran delitos puntuales y personas determinadas;

En **Colombia** se contempla de manera genérica que se podrá intervenir comunicaciones privadas *"para investigar delitos y acusar a los presuntos infractores"*, *así como "para desarrollar actividades de inteligencia y contrainteligencia"*.

Ambas legislaciones presentan criterios muy amplios, subjetivos y ambiguos que vulneran el principio de legalidad, dejándonos en un estado de indefensión al no limitar y acotar el actuar de las autoridades con el fin de evitar afectaciones arbitrarias, caprichosas o abusivas en las esfera jurídica de las personas. En **El Salvador** de la existencia de indicios racionales de que se ha cometido, se está cometiendo o está por cometerse un hecho delictivo.

Países como **Perú**, por su parte, basan la motivación de las medidas más bien en la categoría de delitos que se investigan; es decir, delitos en flagrancia delictiva y delitos graves, como lo son casos de corrupción, terrorismo, secuestro o lavado de dinero.

Sin embargo, si bien a partir de las normas previamente descritas se puede desprender un requisito general de fundamentación y motivación, que incluye constatar elementos objetivos que justifiquen su necesidad y proporcionalidad, resulta dudosa su aplicación tanto en el desarrollo de reglas de procedencia específica en otras leyes secundarias, como en la práctica.

---

112 Constitución Política del Perú, artículo 2.10.
113 Hasta 60 días, prorrogables. Artículos 1, 2.7 y 2.8 Ley N.º 27697.
114 Código Procesal Penal, artículo 231.3 y 228.
115 Constitución Política del Perú, artículo 200.1.
116 Idem, artículo 200.3
117 Decreto Legislativo N° 1182, artículos 3 y Segunda Disposición Complementaria Final.

Por otro lado, a pesar de que la mayoría de las leyes establecen quiénes serán las autoridades facultades para intervenir comunicaciones, hemos detectado una incertidumbre jurídica regional mediante el establecimiento de términos vagos o genéricos con respecto a los supuestos en los que dichas autoridades pueden hacer uso de medidas de vigilancia.

Por ejemplo, en **México**, las Fiscalías pueden ordenar la intervención de comunicaciones cuando *"consideren necesaria"* dicha medida dentro de una carpeta de investigación de un delito.

SOBRE LAS SALVAGUARDAS PARA LA PREVENCIÓN, IDENTIFICACIÓN Y REPARACIÓN DE MEDIDAS DE VIGILANCIA ILEGALES

La mayoría de países objeto de esta investigación establecen la necesidad de un control judicial previo para la intervención de comunicaciones privadas. Sin embargo, algunos países de la región establecen preocupantes excepciones que permiten eludir dicho control judicial.

Por ejemplo, en **Brasil** se permite que, si el tribunal no se pronuncia en el plazo de 12 horas, el Ministerio Público o un agente de policía puedan solicitar los datos directamente a las empresas de telecomunicaciones y telemática. De igual manera, en **México** el mecanismo excepcional establecido en el artículo 303 del Código Nacional de Procedimientos Penales permite a las fiscalías solicitar el acceso a datos conservados o la geolocalización en tiempo real a empresas de telecomunicaciones sin obtener previamente una autorización judicial, en donde la excepción se ha convertido en la regla general y un número importante de solicitudes realizadas bajo el mecanismo excepcional no son ratificadas por la autoridad judicial.

Asimismo, en **Paraguay** se otorga tanto al juez como al Ministerio Público la facultad de requerir informes a personas o entidades públicas o privadas sin autorización judicial; y en **Colombia** el uso de datos de las comunicaciones en la investigación penal[118] y para las funciones de inteligencia[119] no imponen la obligación del control judicial.

En este sentido, se recalca que la elusión del control judicial de medidas de vigilancia fomenta los abusos al desprendernos de requeridos contrapesos, impide la detección de los mismos y permite la impunidad que fomenta su repetición crónica. Por ello, resulta necesario que los marcos jurídicos detallen con claridad la necesidad del control judicial federal previo o inmediato de todas las medidas de vigilancia reconocidas por sus marcos legales, sin mecanismos excepcionales que permitan la elusión de dicho requisito.

Por otro lado, se observa que algunos marcos legales, como el de **Brasil** y **Perú**, contemplan medidas de salvaguarda adicionales para el ejercicio del derecho a la protección de datos personales –como lo es el habeas data– así como la mención de un habeas corpus como recurso efectivo contra casos de abusos.

También se celebra que los marcos legales de **Chile** y **Perú** contemplen el derecho de notificación de las personas afectadas, otorgando un recurso efectivo de acceso a la justicia para las personas frente a potenciales abusos de las medidas de vigilancia. Sin embargo, faltaría analizar –especialmente considerando la falta de transparencia que prevalece en el uso de dichas medidas de vigilancia– en cuántos casos dicha salvaguarda se ha puesto en efecto en práctica.

118 Decreto N.° 1704 de 2012.

119 Ley 1621 de 2013, artículo 44.

El caso de **Chile** es uno de los más protectores en términos de marco legal, estableciendo de manera expresa la excepción de las medidas de interceptación a comunicaciones entre abogado e imputado (igual que en **México**) y ordena a los proveedores de servicios de internet a la destrucción de los datos de sus suscriptores cuando transcurra el plazo máximo de almacenamiento de dicha información.

Se destaca que **ninguno de los países de la región contempla medidas de transparencia estadística ni de supervisión independiente** respecto del uso y alcance de los poderes y técnicas de vigilancia de las comunicaciones empleadas. En este sentido, uno de los problemas principales en el análisis de este tipo de medidas, es que no contamos con suficiente información para comprender el alcance, naturaleza y aplicación de leyes que permitan la vigilancia de las comunicaciones.

Por el contrario, muchas veces la autorización suele recaer en un superior jerárquico de la misma institución solicitante. Esta situación se observa, por ejemplo, en el acceso a información por parte de la ABIN y fuerzas policiales en Brasil; la Ley de la Guardia Nacional en México; la PNP y el OSIPTEL en Perú; y, las Fuerzas Militares, Policía Nacional y Dirección Nacional de Inteligencia en Colombia, lo cual genera preocupaciones por no existir separación entre quien investiga y quien autoriza la medida.

Por lo que, los marcos legales deben prever una institución civil independiente de los servicios de inteligencia y del Poder Ejecutivo, con conocimientos técnicos, para poder fiscalizar a las autoridades facultadas, tanto en cuanto a sus obligaciones de transparencia como en términos de rendición de cuentas.

CAPÍTULO TRES: CASOS DE VIGILANCIA DE COMUNICACIONES EN LA REGIÓN SEGÚN EL TIPO DE VIGILANCIA EMPLEADA

En el siguiente Capítulo se da un breve recuento de casos en los que se detectó el uso de alguna medida de vigilancia de las comunicaciones; a saber: **(I)** casos de intervención de comunicaciones privadas en términos generales, contemplando en la especie: (a) la colaboración de empresas de telecomunicaciones; y (b) la extracción de información; **(II)** el uso de *spywares*; **(III)** la geolocalización basada en la explotación de vulnerabilidades en la infraestructura de telecomunicaciones (SS7); **(IV)** el ciberpatrullaje; y, **(V)** la vigilancia de personas a través de sistemas de lectura de matrículas de automóviles.

Para cada caso, se da una descripción breve sobre la técnica de vigilancia, el tipo de tecnología empleada, las autoridades que hicieron uso de la misma, así como el perfil de las víctimas, en aras de identificar tendencias y patrones en la utilización de medidas de vigilancia en la región latinoamericana.

I. Intervención de comunicaciones privadas

A continuación se presentan ejemplos de intervención de comunicaciones privadas en términos generales (en **Colombia** y **Chile**); así como ejemplos en lo particular de: (a) la colaboración de empresas de telecomunicaciones en el acceso a registro de datos conservados (en **Paraguay**, **Chile** y **México**); y, (b) la extracción de información.

Se precisa que el alcance de lo que debe entenderse como comunicaciones privadas ha ido ampliándose con la evolución y carácter dinámico de la tecnología y que diversos tribunales han interpretado que los datos de tráfico de las comunicaciones o metadatos también se encuentran protegidos por el derecho a la inviolabilidad de las comunicaciones. Consecuentemente, la división realizada tiene como único fin una mejor visualización de distintas maneras de intervenir las comunicaciones privadas.

En este sentido, en cuanto a esta técnica de vigilancia, se contempla una definición amplia del concepto de intervención de comunicaciones privadas, que comprende todo tipo de información y tanto el contenido mismo de las comunicaciones como los metadatos, a los que también se nombra como datos de tráfico de comunicaciones. A su vez, se entiende que el concepto abarca tanto el acceso como el registro, grabación, recolección y almacenamiento de la información, tanto en tiempo real como con posterioridad al momento en que se produce el proceso comunicativo.[120]

También se precisa que la intervención de las comunicaciones, aún cuando se fundamente en facultades conferidas por ley, puede dar lugar a abusos en su aplicación, así como al empleo de tecnologías que vulneren el derecho a la privacidad.

A continuación se presentan dos casos emblemáticos, en términos generales, de intervención de comunicaciones privadas en **Colombia** y **Chile**.

120 Se tomó en cuenta la definición legal del artículo 34, segundo párrafo de la Ley de Seguridad Nacional de México.

COLOMBIA

Por una denuncia de *Revista Semana*,[121] se tuvo conocimiento de que, desde diciembre de 2019 hasta febrero de 2020, el Ejército Nacional realizó actividades de espionaje mediante "un programa de seguimiento informático" que tenía como fin llevar a cabo "perfilamientos" y "trabajos especiales"[122] mediante la recolección de información personal de más de 130 personas.[123] Entre las personas afectadas se encuentran periodistas, ex ministros, funcionarios de Presidencia, generales, políticos, sindicalistas y periodistas estadounidenses.

Dicha vigilancia ilegal fue realizada por el Ejército Nacional, mediante sus batallones de ciberinteligencia (en adelante, "Bacib").[124] Un indicador importante de las irregularidades fueron las alertas emitidas por organismos de inteligencia estadounidense, que señalaron haber identificado el uso para fines ilegales de unos equipos técnicos que ellos mismos habían donado al Ejército colombiano.

En el año 2019, el Ministerio de Defensa, bajo el Ejército Nacional, adquirió el software *Hombre Invisible*,[125] cuyo proveedor era la empresa española *Mollitiam Industries*.[126] El objetivo del contrato era la "adquisición de la plataforma suite de penetración para el desarrollo de las actividades que se llevan a cabo en el campo de la ciberdefensa activa del Ejército Nacional". A la fecha, la información sobre su contratación no se puede consultar de manera abierta en las páginas de contratación estatal.

A raíz de la publicación de la *Revista Semana*, la organización Fundación para la Libertad de Prensa (en adelante, "FLIP") documentó e identificó un total de 52 casos de periodistas vigilados de manera ilegal por el Ejército Nacional para junio de 2020.[127] La FLIP también presentó ante la Fiscalía General de la Nación (en adelante, "FGN") una petición para conocer más información sobre el caso. De acuerdo con lo señalado, la FGN manifestó que no se trató de "130 blancos los objetos de acciones ilegales de monitoreo, seguimientos, interceptaciones, perfilaciones, trabajos especiales por el Ejército Nacional, sino un número de personas que no supera los 20".[128]

---

121 Semana. (2020). Espionaje del Ejército Nacional: Las carpetas secretas. Disponible en: https://www.semana.com/nacion/articulo/espionaje-del-ejercito-nacional-las-carpetas-secretas-investigacion-semana/667616/

122 De acuerdo con la terminología usada por los militares.

123 Por ejemplo, teléfonos, direcciones de residencia y trabajo, correos electrónicos, amigos, familiares, hijos, colegas, contactos, infracciones de tráfico y hasta lugares de votación – de diversas personas.

124 Estos "pertenecen a las brigadas de inteligencia militar y al Batallón de Contrainteligencia de Seguridad de la Información (Bacsi). Ambos dependen del Comando de Apoyo de Inteligencia Militar (Caimi) y del Comando de Apoyo de Contrainteligencia Militar (Cacim)".
Durante el periodo de diciembre de 2019, el Ministro de Defensa era Carlos Holmes Trujillo y el comandante del Ejército era Nicacio Martínez. El primero de los dos, Ministro de Defensa en los primeros años de la administración de Iván Duque; y el segundo, excomandante del Ejército que anunció su retiro en el mismo periodo que la Corte Suprema de Justicia allanó dicha entidad. Para mayo de 2020, fecha en la que se publican el artículo de Semana sobre las denominadas "carpetas secretas", el comandante del Ejército era Eduardo Zapateiro. De acuerdo con la revista Semana, estos cambios de mando se dan en relación con el descubrimiento sobre las irregularidades en materia de vigilancia digital que se dieron a manos del Ejército a finales de 2019.

125 Rico, M. (2023, febrero 20). Mollitiam: así es la contratista del Ejército y sus herramientas de ciberespionaje. Disponible en: https://www.elespectador.com/judicial/mollitiam-asi-es-la-contratista-del-ejercito-y-sus-herramientas-de-ciberespionaje/

126 Mollitiam Industries. https://www.mollitiamindustries.com/ (Contrato adjudicado mediante el proceso No. 277-CENAINTELIGENCIA 2019.

127 Fundación para la Libertad de Prensa (FLIP). (2020). Catorce nuevos casos de periodistas que fueron víctimas de acciones de perfilamiento por parte del Ejército Nacional. Disponible en: https://flip.org.co/en/pronunciamientos/catorce-nuevos-casos-de-periodistas-que-fueron-victimas-de-acciones-de-perfilamiento-por-parte-del-ejercito-nacional

128 Fundación para la Libertad de Prensa. (2020). Cuatro meses después de las carpetas secretas.
Disponible en: https://flip.org.co/en/pronunciamientos/cuatro-meses-despues-de-las-carpetas-secretas

Luego de la publicación de la denuncia, algunas víctimas manifestaron haber experimentado violencia o represalias relacionadas con el caso. Un ejemplo fueron los periodistas de *Rutas del Conflicto* (en adelante, ''RdC''), un proyecto de periodismo que documenta hechos relacionados con el conflicto armado en el país. De acuerdo con Óscar Parra, miembro del equipo de RdC, a pesar de no tener pruebas que relacionen los hechos, consideran que el inicio de su "perfilación" como organización surgió de una solicitud de información al Ejército Nacional en el marco de una investigación adelantada por RdC en 2019.[129]

Según lo expuesto por O. Parra, luego de realizar dicha solicitud y tener que insistir mediante instancias judiciales, dos militares se presentaron en la oficina de la organización para responder personalmente a la misma, evitando dar respuesta mediante correo físico o digital. Asimismo, los oficiales se quedaron fuera del edificio ese mismo día.

A la luz de lo ocurrido, Parra calificó esto como una intimidación sobre la que informaron al juez que llevaba el caso y que al final le ordenó al Ejército que diera la información correspondiente. De igual forma, el general Nicacio Martínez presentó una tutela[130] contra el mismo periodista, argumentando que RdC estaba desprestigiando al Ejército. La justicia falló a favor de RcD y cerró el proceso.

Si bien éste es uno de los pocos relatos relacionados con algún tipo de represalia adicional a las medidas de vigilancia denunciadas por *Revista Semana*, es importante resaltar que las personas periodistas en Colombia son constantemente blanco de estas actuaciones de vigilancia ilegal y ven vulnerado su derecho a la libertad de expresión y privacidad con mayor frecuencia que otros sectores. Desde el año 2019, la FLIP ha documentado un número elevado de agresiones contra periodistas, con una tendencia sostenida de entre 400 y 500 ataques anuales en Colombia.[131]

Después de que se conocieran las acciones de vigilancia ilegal, se iniciaron dos investigaciones, una por la Procuraduría General de la Nación (en adelante, ''PGN'') y otra por la FGN. De acuerdo con el medio *El Espectador*,[132] para 2021, la investigación más adelantada era la de la PGN, en la cual se "mandó formular pliego de cargos a militares con pruebas de los equipos, las personas, las órdenes y la información recuperada".[133]

No obstante, para febrero de 2021, el mismo medio de comunicación señaló que las investigaciones de ambas entidades no fueron coincidentes en cuanto al número de personas víctimas de dichas acciones ilegales. Asimismo, se indicó que para esa fecha *"se desconocían los avances en el proceso disciplinario y la formulación de pliego de cargos establecido por la Procuraduría a trece militares y la audiencia pública que debía suceder"*.[134]

---

129 Abu Shihab, L. (2020, mayo 5). Hablamos con una de las víctimas de espionaje por parte del Ejército colombiano. VICE. https://www.vice.com/es/article/nuevo-escandalo-en-colombia-por-seguimientos-ilegales-del-ejercito-a-periodistas-politicos-y-defensores-de-derechos-humanos/

130 La acción de tutela es un mecanismo establecido en el artículo 86 de la Constitución Política de la República de Colombia. La acción de tutela consiste en la facultad que tiene toda persona en poder reclamar ante un juez, en todo momento y lugar, mediante un procedimiento preferente y sumario, la protección judicial inmediata de sus derechos constitucionales fundamentales.

131 El Colombiano. (2024). La violencia contra los periodistas se disfraza como el derecho a debatir de los gobernantes. Disponible en: https://www.elcolombiano.com/colombia/la-violencia-contra-los-periodistas-se-disfraza-como-el-derecho-a-debatir-de-los-gobernantes-flip-OH23715128

132 El Espectador. (2021). "Carpetas secretas".: Después de la denuncia, el silencio. Disponible en: https://www.elespectador.com/judicial/carpetas-secretas-despues-de-la-denuncia-el-silencio-article/

133 Esto se ordenó para el 20 de mayo de 2020 contra trece militares, entre los que se incluyeron los generales Eduardo Quirós y Gonzalo Ernesto García, quienes van a enfrentar juicio disciplinario en la Procuraduría. El último de ellos, fue funcionario del extinto Departamento Administrativo de Seguridad, disuelto tras el escándalo de las "chuzadas" en el gobierno de Álvaro Uribe.

134 El Espectador. (2021). "Carpetas secretas".: Después de la denuncia, el silencio. Disponible en: https://www.elespectador.com/judicial/carpetas-secretas-despues-de-la-denuncia-el-silencio-article/

Aparte de las medidas tomadas por las entidades nacionales, en octubre de 2020, la CIDH convocó una audiencia pública sobre el caso.[135] "La delegación del Estado colombiano, encabezada por Alejandro Ordóñez, embajador ante la OEA, negó el carácter sistemático de estas actividades. También afirmó que, para la fecha de la audiencia, "había nueve investigaciones abiertas por estos hechos, negando además la falta de participación de las víctimas". Esta audiencia no se encuentra en los registros audiovisuales de la CIDH y no es claro identificar las nueve investigaciones a las que se refirió Ordoñez. En la audiencia se recalcó lo siguiente:

> La problemática de la inteligencia ilegal en Colombia, [para ese entonces, ya había] ocupado a la CIDH por dieciséis años durante los cuales han persistido la impunidad y la falta de información sobre el contenido de estas actividades ilegales, así como la falta de esclarecimiento sobre las motivaciones y la estructura que opera detrás de las interceptaciones y la repetición de los hechos.[136]

CHILE

En octubre de 2019, se reveló la filtración de miles de archivos de inteligencia desplegados por la institución policial Carabineros de Chile, donde se evidenciaba el seguimiento ilegal a las comunicaciones de dirigentes sociales, movimientos de defensoras de derechos humanos y sindicatos en el país.[137]

Las filtraciones, denominadas *PacoLeaks*[138], se publicaron los días 25, 26 y 28 de octubre de 2019.[139] La tercera filtración reveló datos de más de 300 memos internos y 10.000 archivos adjuntos de Carabineros, con información detallada sobre actividades de movimientos sociales y sindicatos,[140] así como informes de seguimiento y vigilancia a líderes y sus organizaciones.[141] En esta línea, se evidenció que los movimientos ambientales y los grupos feministas son el objetivo principal de las labores de inteligencia de Carabineros.

Si bien en este caso no se pudo identificar la identidad del operador de la tecnología de vigilancia, desarrollador u intermediarios que permitieron la extracción de la información, a raíz de esta filtración de archivos de inteligencia se conocieron diversos mecanismos de vigilancia y espionaje de la institución policial en cuestión contra organizaciones sociales. Según una de las fuentes consultadas,[142] entre dichos mecanismos destacan: búsqueda de actividad e intercambio de comunicaciones en redes sociales, infiltración en eventos, seguimiento *in situ* de manifestantes y dirigentes, registro fotográfico policial en primera persona, espionaje vía drones y fichas de reconocimiento con datos personales.

---

135 Comisión Colombiana de Juristas. (2020). CIDH reiteró que la vigilancia ilegal en Colombia es sistemática y pidió garantías para las víctimas. Disponible en: https://www.coljuristas.org/sala_de_prensa/cidh-reitero-que-la-vigilancia-ilegal-en-colombia-es-sistematica-y-pidio-garantias-para-las-victimas

136 Ibídem.

137 CIPER (2019). Hackeo a Carabineros en medio de la crisis expone 10.515 archivos: entre ellos hay datos de inteligencia. Disponible en: https://www.ciperchile.cl/2019/10/29/hackeo-a-carabineros-en-medio-de-la-crisis-expone-10-515-archivos-entre-ellos-hay-datos-de-inteligencia/

138 Paco, término ampliamente utilizado en Chile para referirse a los agentes de policía.

139 La Izquierda Diario (2019). PACOLEAKS. Filtración de documentos de Carabineros revela seguimientos a organizaciones políticas y sociales. Disponible en: https://www.laizquierdadiario.com/Filtracion-de-documentos-de-Carabineros-revela-seguimientos-a-organizaciones-politicas-y-sociales

140 Huelgas legales, negociaciones colectivas, actos de "pintatón", puntos de prensa o actos públicos.

141 Interferencia (2019). PacoLeaks: Estos son los nombres y organizaciones que han sido vigiladas por Carabineros en los últimos meses. Disponible en: https://interferencia.cl/articulos/pacoleaks-estos-son-los-nombres-y-organizaciones-que-han-sido-vigiladas-por-carabineros-en

142 Doble Espacio (2019). De las Juventudes Comunistas a la Universidad Católica: las organizaciones e instituciones investigadas por Carabineros. Disponible en: https://doble-espacio.uchile.cl/2019/11/04/desde-las-juventudes-comunistas-a-la-universidad-catolica-las-organizaciones-e-instituciones-investigadas-por-carabineros/

De acuerdo con algunos medios de comunicación,[143] entre las organizaciones sociales, dirigentes y movimientos defensores de derechos humanos que figuraban en los documentos de seguimiento e inteligencia, se encontraban: gremios y sindicatos como el Colegio de Profesores, Agrupación Nacional de Empleados Fiscales (en adelante "ANEF"), Confusam y la Central Unitaria de Trabajadores (en adelante, "CUT"); organizaciones estudiantiles como la Federación de Estudiantes de la Universidad de Chile (en adelante, FECH) y la Federación de Estudiantes de la Universidad Arturo Prat (en adelante, "FEDEUNAP"); y, colectivos de derechos humanos como la Agrupación de Familiares de Detenidos Desaparecidos (en adelante, "AFDD"), Agrupación de Familiares Ejecutados Políticos (en adelante, "AFEP") y la Coordinadora Nacional de Organizaciones de Derechos Humanos y Sociales. También figuran movimientos sociales y temáticos como No+AFP, Modatima, No a Ciclo y el Movimiento por el Agua y los Territorios, así como agrupaciones feministas como la Red Chilena Contra la Violencia hacia las Mujeres, la Red de Mujeres del Norte y el Colectivo Voz en Fuga.

Además, se conocieron fichas con fotografías, datos personales y, en algunos casos, movimientos detallados de líderes sociales catalogados como "blancos de interés",[144] entre los que figuran Rodrigo Mundaca, líder de Modatima; Bárbara Figueroa, presidenta de la CUT; Mario Aguilar, del Colegio de Profesores; Luis Mesina, vocero de la Coordinadora No+AFP; y Emilia Schneider, presidenta interina de la FECH.

Carabineros de Chile ratificó la veracidad de los documentos filtrados justificando su accionar en la Ley de Inteligencia y en la protección de la seguridad pública e integridad física de los convocantes a actividades sociales.[145]

En el caso del líder de Modatima, la información filtrada detalla la hora exacta de su llegada a Chile el 1 de octubre de 2019, luego de recibir el Premio Internacional de Derechos Humanos de Nüremberg, Alemania. El dirigente señaló que fue amenazado de muerte, de manera anónima, a través de redes sociales luego de su llegada al país.[146] Para el líder ambiental, la información de Carabineros sobre su llegada a Chile:

> (...) da cuenta de lo que hemos denunciado desde hace mucho tiempo, hay una acción coordinada por parte de fuerzas de inteligencia de estado [...] chequear todos los pasos que damos, estar en permanente vigilancia, lo cual atenta contra derechos humanos fundamentales, el derecho a la libertad, a la libre opinión, derecho a disentir.[147]

Sumado a lo anterior, Emilia Schneider, presidenta interina de la FECH, manifestó que *"es preocupante que nos cataloguen como blanco de interés, más cuando vemos dirigentes que han sido asesinados como Macarena Valdés o Camilo Catrillanca"*[148]. Luego de las filtraciones, varias organizaciones sociales dieron a conocer a los medios de comunicación sobre el monitoreo de Carabineros a actividades que no tenían convocatoria multitudinaria.

---

143 Interferencia (2019). PacoLeaks: Estos son los nombres y organizaciones que han sido vigiladas por Carabineros en los últimos meses. Disponible en: https://interferencia.cl/articulos/pacoleaks-estos-son-los-nombres-y-organizaciones-que-han-sido-vigiladas-por-carabineros-en

144 Interferencia (2019). PacoLeaks: Carabineros creó fichas de líderes sociales para mantenerlos vigilados. Disponible en: https://interferencia.cl/articulos/pacoleaks-carabineros-creo-fichas-de-lideres-sociales-para-mantenerlos-vigilados

145 Interferencia (2019). PacoLeaks: Estos son los nombres y organizaciones que han sido vigiladas por Carabineros en los últimos meses. Disponible en: https://interferencia.cl/articulos/pacoleaks-estos-son-los-nombres-y-organizaciones-que-han-sido-vigiladas-por-carabineros-en

146 Interferencia (2020). Habla Mundaca sobre el rechazo de la Suprema a su amparo por 'Pacoleaks': "es un voto de confianza a una policía que viola los DD.HH." Disponible en: https://interferencia.cl/articulos/habla-mundaca-sobre-el-rechazo-de-la-suprema-su-amparo-por-pacoleaks-es-un-voto-de

147 Interferencia (2019). PacoLeaks: Estos son los nombres y organizaciones que han sido vigiladas por Carabineros en los últimos meses. Disponible en: https://interferencia.cl/articulos/pacoleaks-estos-son-los-nombres-y-organizaciones-que-han-sido-vigiladas-por-carabineros-en

148 Interferencia (2019). PacoLeaks: Carabineros creó fichas de líderes sociales para mantenerlos vigilados. Disponible en: https://interferencia.cl/articulos/pacoleaks-carabineros-creo-fichas-de-lideres-sociales-para-mantenerlos-vigilados

En 2019, a raíz de las filtraciones de los archivos de inteligencia, se iniciaron múltiples acciones legales contra Carabineros y el Ministerio del Interior.[149] Por ejemplo, el Colegio de Profesores presentó un recurso de amparo en contra del director general de Carabineros, Mario Rozas, y del ministro del Interior, Gonzalo Blumel.[150]

El recurso de amparo fue rechazado por la Corte de Apelaciones de Santiago bajo el siguiente argumento:

> (...) que para que puedan ser valorados los antecedentes traídos al conocimiento del tribunal, éstos deben haber tenido un origen legítimo y ajustado a derecho; y de no ser así, no pueden ser tomados en consideración ni validados en un procedimiento jurisdiccional [...] este recurso tiene como fundamento un hecho antijurídico, como lo es el hackeo y extracción de información de Carabineros de Chile, respecto del cual la institución afectada ha formulado – según ha expresado – el consiguiente requerimiento en sede penal.[151]

El líder de Modatima también presentó un recurso de amparo contra el Director General de Carabineros y el Ministro del Interior, solicitando precisar desde cuando se realizaban las prácticas de vigilancia y *"el propósito de analizar lo que hacemos, qué pensamos, con quienes nos juntamos"*.[152] La Corte de Apelaciones de Santiago también rechazó el recurso de amparo bajo el mismo argumento que en el caso del Colegio de Profesores.[153]

En este mismo sentido, la vicerrectora de Extensión y Comunicaciones de la Universidad de Chile, la presidenta de la Agrupación de Familiares de Detenidos Desaparecidos, la presidenta de la FECH y otros activistas, presentaron una querella contra el Ministro del Interior y el Director General de Carabineros por el espionaje realizado en su contra[154]. Este recurso también fue rechazado con el argumento de los casos anteriores sobre el origen de los antecedentes traídos al conocimiento del tribunal.[155]

149 Interferencia (2019). Dirigentes sociales vigilados toman acciones legales contra Rozas y Blumel. Disponible en: https://interferencia.cl/articulos/dirigentes-sociales-vigilados-toman-acciones-legales-contra-rozas-y-blumel

150 Para más información, ver: https://juris.pjud.cl/busqueda/pagina_detalle_sentencia?k=eHFSeVBncXp0Z085dzhVU2M-veThnQT09

151 COLEGIOS DE PROFESORES DE CHILE A.G / CARABINEROS DE CHILE - MINISTERIO DEL INTERIOR VISTA EN POS DEL ING. CORTE 2460-2019: 09-12-2019 (-), Rol N° 2473-2019. En Buscador Corte de Apelaciones (https://juris.pjud.cl/busqueda/u?7ps0). Fecha de consulta: marzo de 2025

152 Interferencia (2020). Habla Mundaca sobre el rechazo de la Suprema a su amparo por 'Pacoleaks': "es un voto de confianza a una policía que viola los DD.HH." Disponible en: https://interferencia.cl/articulos/habla-mundaca-sobre-el-rechazo-de-la-suprema-su-amparo-por-pacoleaks-es-un-voto-de

153 MUNDACA CABRERA RODRIGO / CARABINEROS DE CHILE VISTA CON ING. CORTE 2319, 2362, 2460, 2473, 2507, 2512 Y 2682 TODAS DEL 2019.-: 09-12-2019 (-), Rol N° 2295-2019. En Buscador Corte de Apelaciones (https://juris.pjud.cl/busqueda/u?7psz). Fecha de consulta: marzo de 2025

154 Interferencia (2019). Dirigentes sociales vigilados toman acciones legales contra Rozas y Blumel. Disponible en: https://interferencia.cl/articulos/dirigentes-sociales-vigilados-toman-acciones-legales-contra-rozas-y-blumel

155 OLIVARES SAAVEDRA ROSARIO-ASTUDILLO ASTUDILLO LEANDRO-BARRA ARANCIBIA GUILLERMO-SCHNEIDER VIDELA EMILIA/MINISTERIO DEL INTERIOR Y SEGURIDAD PUBLICA-CARABINEROS DE CHILE. VISTA EN POS DEL ING. CORTE 2507-2019.-: 09-12-2019 (-), Rol N° 2512-2019. En Buscador Corte de Apelaciones (https://juris.pjud.cl/busqueda/u?7hgt). Fecha de consulta: marzo de 2025

II. Colaboración de empresas de telecomunicaciones en el acceso a registro de datos conservados

Como observó el entonces Alto Comisionado de las Naciones Unidas para los Derechos Humanos en su informe de 2014 sobre "El derecho a la privacidad en la era digital", tanto el contenido de las comunicaciones como sus metadatos están protegidos por el derecho a la privacidad, ya que los metadatos también pueden revelar datos sobre el comportamiento de las personas y permitir extraer conclusiones sobre su vida privada.[156]

En este sentido, la conservación y almacenamiento de los metadatos de las comunicaciones por parte de las empresas de telecomunicaciones suele formar parte de las medidas legislativas y de política pública en materia de colaboración con la justicia, principalmente para que las autoridades puedan solicitar su acceso, mediante autorización judicial previa, con fines de prevención e investigación de delitos.

No obstante, la mayoría de los marcos legales que regulan dicho acceso no establecen de manera clara y precisa cuáles son las autoridades que podrán tener acceso a dichos datos personales, en qué circunstancias, bajo qué procedimientos y con qué salvaguardas. Lo anterior es particularmente preocupante considerando que dicha práctica consiste en la conservación masiva e indiscriminada de los datos personales de millones de usuarias de servicios de telefonía móvil, la mayoría de las cuales no se encuentran, ni encontrarán, implicadas en la comisión de un delito.

En este sentido, se han detectado graves irregularidades y abusos en la región en cuanto al acceso de dichos datos. A continuación se ejemplifica su utilización con casos documentados en **Paraguay, Chile y México.**

PARAGUAY

En Paraguay, el Ministerio Público puede solicitar acceder a los metadatos de las comunicaciones que conservan los proveedores de Internet sin autorización judicial y sin que exista una causa formal o imputación previa, simplemente por estar investigando un caso y considerarlo necesario.[157]

Actualmente, hay más de 20 casos ante la Corte Suprema de Paraguay que cuestionan este procedimiento. Sin embargo, desde 2004, la Corte ha mantenido su postura, considerando que los metadatos no forman parte de las comunicaciones y, por lo tanto, pueden ser solicitados por el Ministerio Público sin orden judicial.[158]

156 Naciones Unidas. Asamblea General. (2014). Resolución A/HRC/27/37. El derecho a la privacidad en la era digital, Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. Párr. 19. Disponible en: https://docs.un.org/es/A/HRC/27/37

157 Con base en el artículo 228 del Código Procesal Penal.

158 Para más información, ver resumen "Quien defiende tus datos" (todas las ediciones), en donde la ISP TIGO facilita la cantidad de solicitudes de informes que realiza anualmente la fiscalía. También véase: https://www.tedic.org/wp-content/uploads/2025/02/QDTD_Paraguay_2024-WEB.pdf

CHILE

En el marco del estallido social y político de 2019, la Fiscalía Metropolitana Occidente de Chile,[159] solicitó a los proveedores de servicios de internet (ISPs) la entrega de datos de las personas abonadas a servicios de telefonía móvil que circularon en las inmediaciones de las estaciones quemadas del Metro.[160] En dicha solicitud, se requería el acceso a la totalidad de números telefónicos que se conectaron a las antenas y celdas de *Entel*, *Movistar y WOM* entre el 18 y 28 de octubre cerca de 5 estaciones de Metro en la zona occidente de Santiago.[161]

La Fiscalía elevó la solicitud en dos ocasiones, el 4 y el 12 de noviembre del año 2019. En la primera, solicitó a través de la Brigada de Investigaciones Policiales Especiales (en adelante, ''BIPE'') de la Policía de Investigaciones de Chile (en adelante, ''PDI'') a *Entel*, *Movistar* y *WOM* la entrega de información del tráfico de las antenas telefónicas instaladas entre las comunas de Maipú y Pudahuel, donde se registraron los ataques a estaciones de Metro.

Según reportes realizados por el medio *La Tercera*[162], *WOM* fue la única compañía que dio la información en la primera petición, sin que mediara una orden judicial necesaria prevista por ley[163] para autorizar dicha entrega. *Movistar* se negó y *Entel* entregó los datos de manera parcial.

A raíz de lo anterior, ocurrió el segundo requerimiento, donde la Fiscalía hizo una solicitud ante el Noveno Juzgado de Garantía de Santiago, pidiendo al tribunal una orden judicial general para que *Entel* y *Movistar* entregarán la información requerida por el Ministerio Público[164]. El 12 de noviembre el tribunal ordenó la entrega de los datos sobre la totalidad de teléfonos móviles que se conectaron a las antenas de dichas compañías telefónicas en las estaciones atacadas.

Al respecto, WOM emitió un comunicado manifestando que:

> Requirió mayor precisión de la solicitud enviada por el organismo y una vez recibida la aclaración se procedió a dar cumplimiento de la orden judicial remitida por el Ministerio Público. Esta información sólo se refiere a los tráficos sobre nuestras antenas, lo que no implica datos específicos de los clientes.[165]

Según una consulta de CIPER Chile a la Fiscalía en 2023,[166] seis personas fueron condenadas por los ataques a las estaciones de Metro en la zona occidente de Santiago. A la fecha, no se ha establecido una correlación entre su condena y la petición de información de la Fiscalía a las compañías de telefonía móvil.

---

159 BioBioChile (2020). Fiscalía solicitó datos a empresas móviles para identificar a quienes atacaron estaciones del Metro. Disponible en: https://www.biobiochile.cl/noticias/ciencia-y-tecnologia/moviles-y-computacion/2020/01/08/afirman-que-wom-entrego-informacion-de-usuarios-durante-estallido-social-compania-se-defendio.shtml

160 Las medidas de vigilancia presentadas responden a un caso de geofence. Esto consiste en la solicitud por parte de las autoridades de los datos de localización e identificación inversa de las personas que estuvieron circulando cerca a ciertas estaciones del Metro de Santiago que habían sido quemadas.

161 La Tercera (2019). Fiscalía pide levantar información de antenas celulares de los días en que ocurrieron ataques al Metro. Disponible en: https://www.latercera.com/nacional/noticia/fiscalia-pide-levantar-informacion-antenas-celulares-dias-ocurrieron-ataques-al-metro/963909/

162 La Tercera (2020). WOM por entrega de información a fiscalía por ataque a Metro: "No implica datos específicos de los clientes". Disponible en: https://www.latercera.com/nacional/noticia/wom-entrega-informacion-fiscalia-ataque-metro-no-implica-datos-especificos-los-clientes/966760/

163 Consagrado en el artículo 19 de la Ley 21732.

164 La Tercera (2019). Fiscalía pide levantar información de antenas celulares de los días en que ocurrieron ataques al Metro. Disponible en: https://www.latercera.com/nacional/noticia/fiscalia-pide-levantar-informacion-antenas-celulares-dias-ocurrieron-ataques-al-metro/963909/

165 La Tercera (2020). WOM por entrega de información a fiscalía por ataque a Metro: "No implica datos específicos de los clientes". Disponible en: https://www.latercera.com/nacional/noticia/wom-entrega-informacion-fiscalia-ataque-metro-no-implica-datos-especificos-los-clientes/966760/

166 CIPER (2023). Fiscalía cerró las causas por ataques al Metro: condenó a 14 personas y no detectó grupos organizados para quemar estaciones. Disponible en: https://www.ciperchile.cl/2023/10/17/fiscalia-cerro-las-causas-por-ataques-al-metro-condeno-a-14-personas-y-no-detecto-grupos-organizados-para-quemar-estaciones/

MÉXICO

En México, el artículo 190, fracción II, de la Ley Federal de Telecomunicaciones y Radiodifusión (en adelante, "LFTR")[167] establece la obligación de los concesionarios de telecomunicaciones de conservar, por dos años, un registro de los metadatos de comunicaciones de todos sus usuarios de manera indiscriminada. Este registro incluye metadatos como: el origen y destino de las comunicaciones; su fecha, hora y duración; datos de identificación de los comunicantes y los dispositivos; e incluso la localización geográfica aproximada de los usuarios.

El artículo 190, fracción III de la LFTR establece a su vez la obligación de entrega de datos conservados a las autoridades facultadas para acceder a dicho registro. En este sentido, por solicitudes de acceso a la información, R3D: Red en Defensa de los Derechos Digitales, detectó que existen serias discrepancias entre el número de accesos reportados por las autoridades facultadas, el poder judicial federal y las empresas de telecomunicaciones, sugiriendo una práctica generalizada de acceso ilegal a los datos conservados por empresas de telecomunicaciones.

Adicionalmente, existe evidencia de que el mecanismo excepcional contemplado en el artículo 303 del CNPP, por el cual autoridades pueden solicitar directamente el acceso a los datos, sin control judicial previo, ha sido sistemáticamente abusado para obtener dicha información sin control judicial alguno.

Entre los abusos que se han documentado, se encuentra evidencia revelada por *The New York Times* en noviembre de 2023 sobre cómo la Fiscalía General de Justicia de la Ciudad de México accedió a registros telefónicos, mensajes de texto y datos de localización de diversas figuras políticas, tanto del partido gobernante como de la oposición.[168]

La Fiscalía solicitó esta información a la empresa de telecomunicaciones *Telcel*, argumentando que estos datos serían utilizados en investigaciones sobre secuestros y desapariciones forzadas e invocando las causales de excepción de la autorización judicial previa a las que se refiere el artículo 303 del CNPP.

De acuerdo con *The New York Times*, entre las personas vigiladas desde 2021 hasta la fecha se encuentran Dolores Igareda, alta funcionaria de la Suprema Corte de Justicia de la Nación; Ricardo Amezcua, integrante de la judicatura de la Ciudad de México; Santiago Taboada, alcalde y aspirante a la jefatura de gobierno de la capital; Higinio Martínez, senador de Morena por el Estado de México; Horacio Duarte, entonces titular de la Agencia Nacional de Aduanas; la senadora Lilly Tellez y la ex legisladora Alessandra Rojo de la Vega. De acuerdo con el diario, ninguna de las personas estuvo involucrada en casos de secuestro.

Este *modus operandi* de las autoridades también fue denunciado en 2019 por la periodista Marcela Turati; la cofundadora del Equipo Argentino de Antropología Forense (EAAF), Mercedes Doretti, y la defensora de derechos humanos Ana Lorena Delgadillo. Las mismas señalaron que la Subprocuraduría Especializada en Investigación de Delincuencia Organizada (en adelante, "SEIDO") de México accedió a sus registros telefónicos al incluirlas en en la misma carpeta donde se investigaba a integrantes de una organización delictiva.[169]

---

167 Ley Federal de Telecomunicaciones y Radiodifusión, disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR.pdf – próxima a reformarse, por lo que los artículos 189 y 190 ahora serán los artículos 160 y 161 de la nueva ley.

168 Maria Abi-Habib, Natalie Kitroeff y Emiliano Rodríguez Mega (2023). Políticos y funcionarios, blanco de vigilancia en México. https://www.nytimes.com/es/2023/11/09/espanol/mexico-vigilancia-fiscalia-telcel.html

169 R3D. (2021). SEIDO accedió a registros telefónicos para espiar a periodista y defensoras por investigar masacre de San Fernando. Disponible en: https://r3d.mx/2021/11/26/seido-accedio-a-registros-telefonicos-para-espiar-a-periodista-y-defensoras-por-investigar-masacre-de-san-fernando/

La SEIDO investigó a Turati, Delgadillo y Doretti por los delitos de desaparición forzada y secuestro. De este modo, las autoridades accedieron a su información personal, los teléfonos que usaron y su ubicación geográfica. En el caso de Turati, además obtuvieron los datos personales que entregó a la Secretaría de Relaciones Exteriores para tramitar su pasaporte.

Cabe precisarse que el acceso a datos conservados se realizó sin autorización judicial y que bajo ninguna circunstancia puede considerarse justificado el acceso a dicha información en tanto no existe indicio alguno de que la periodista, defensora y perito, respectivamente, hayan participado en la comisión de delito alguno, sino que su participación en dicho caso consistía exclusivamente en el acompañamiento a las familias de las víctimas denunciantes.

A partir de estos casos se ha apreciado un *modus operandi* en México en el que las fiscalías abren una investigación o usan una existente y, con base en "información anónima", solicitan a las empresas de telecomunicaciones que les den información de números que no guardan relación con algún delito. De esta forma se utilizan carpetas sobre secuestro u otros delitos graves con la intención de eludir la obligación de obtener autorización judicial federal de manera previa.

Además, en ningún caso someten a ratificación judicial las solicitudes de acceso a datos conservados, contraviniendo lo establecido en el artículo 303 del CNPP. Para ello, argumentan que no encontraron utilidad en la información y por ello no tenía sentido solicitar la ratificación judicial, por lo que, de manera imposible de comprobar procedieron a su destrucción.

El esquema documentado sugiere que podrían existir muchos más casos en los que autoridades han obtenido de las empresas de telecomunicaciones, metadatos de comunicaciones y la geolocalización en tiempo real de manera fraudulenta, sin que se lleven a cabo investigaciones que permitan identificar a otras víctimas y sancionar a los responsables.

III. Extracción de información

Dentro del género de intervención de comunicaciones privadas, otras tecnologías de intervención de comunicaciones detectadas en la región son las herramientas de extracción forense.

Estas herramientas permiten extraer de un dispositivo físico toda la información almacenada, incluyendo comunicaciones privadas, datos de identificación de las comunicaciones, así como de la información, documentos, archivos de texto, audio, imagen o video contenidos en cualquier dispositivo, accesorio, aparato electrónico, equipo informático, aparato de almacenamiento y todo aquello que pueda contener información, incluyendo la almacenada en las plataformas o centros de datos remotos vinculados con éstos.[170]

También permiten la clonación de SIM cards, extracción de contraseñas, la recuperación de información borrada e inclusive en algunos casos permite conocer el contenido de aplicaciones de mensajería como Whatsapp, iMessage, entre otras.

La empresa israelí *Cellebrite* es la desarrolladora de la herramienta de extracción forense más popular en el mundo. Por años se ha documentado la comercialización de estos productos a decenas de gobiernos, incluyendo regímenes autocráticos u opresivos de países como China, Turquía, Venezuela, Bielorrusia, Rusia y Bangladesh. Estos gobiernos han utilizado dichos equipos para vigilar injustificadamente a disidentes, periodistas, activistas, personas de la comunidad LGBTIQ+ y personas pertenecientes a minorías étnicas.[171]

---

170 Se tomó en cuenta la definición legal del artículo 291 den CNPP, párr. 4, reformado el 17 de junio de 2016.

171 Access Now. (2021). What spy firm Cellebrite can't hide from investors. Disponible en: https://www.accessnow.org/what-

A partir de la polémica alrededor del abuso de los equipos vendidos por *Cellebrite* y de su interés por cotizar en la bolsa de valores, la empresa declaró que formaría un comité de ética y dejaría de vender sus productos a gobiernos autoritarios u opresores. Sin embargo, extrabajadores de la empresa han declarado que la misma no ha hecho nada para prevenir abusos.[172] Los casos en los que ha actuado ante abusos ha sido hasta que éstos llegan a los medios o hasta que son obligados a actuar a partir de procesos legales.[173]

MÉXICO

En México, decenas de autoridades federales y estatales han adquirido herramientas de extracción forense desarrolladas por *Cellebrite* y otras compañías similares. En muchos casos, la legalidad de su utilización es cuestionable y en la mayoría de los casos existe una extendida opacidad respecto de su uso.[174]

PARAGUAY

En Paraguay existe evidencia de que el Ministerio Público y la Policía Nacional han utilizado *Septier*, según los datos de contrataciones públicas en, por lo menos, el año 2018 en el gobierno del Presidente Mario Abdo Benitez mediante la empresa *Winner*.[175]

IV. Spyware

Una de las tecnologías de vigilancia más invasivas que se han detectado es el uso de sistemas de vigilancia conocidos como *spyware*. Aunque las características pueden variar, típicamente la infección de un dispositivo mediante la operación de un *spyware* permite la interceptación y recopilación indiscriminada de todo tipo de comunicaciones y datos, cifrados o no, así como el acceso remoto y secreto a los dispositivos personales y los datos almacenados en ellos, lo que facilita la vigilancia en tiempo real y la manipulación de los datos contenidos en esos dispositivos.[176] Es decir, la tecnología empleada por un *spyware* da a sus usuarios no sólo la habilidad de monitorear a la persona, sino también de manipular el dispositivo infectado, incluyendo la alteración, borrado o, incluso, implantación de información incriminante.

Una vez infectado un dispositivo, típicamente los operadores del *spyware* podrán grabar comunicaciones de video y audio; recopilar mensajes, textos y correos electrónicos (incluso de plataformas supuestamente seguras); así como acceder a calendarios, contactos y datos de geolocalización. También pueden acceder a otros dispositivos conectados, como los dispositivos tecnológicos vestibles o vehículos, que pueden contener más datos relativos a la salud y la localización de la persona.[177]

---

spy-firm-cellebrite-cant-hide-from-investors/

172 Haaretz. (2021). I worked at Israeli phone hacking firm Cellebrite. They lied to us. Disponible en: https://www.haaretz.com/israel-news/2021-07-27/ty-article/i-worked-at-israeli-phone-hacking-firm-cellebrite-they-lied-to-us/0000017f-f652-d460-afff-ff764fae0000

173 Dhaka Tribune. (2021). Israeli phone-hacking firm Cellebrite to stop sales to Bangladesh. Disponible en: https://www.dhakatribune.com/world/middle-east/255655/israeli-phone-hacking-firm-cellebrite-to-stop

174 Red en Defensa de los Derechos Digitales (R3D). (2025). El Estado de la Vigilancia. Disponible en: https://r3d.mx/wp-content/uploads/EDLV_2025.pdf https://r3d.mx/wp-content/uploads/EDLV_2025.pdf

175 Vinner SRL. Ver: https://winner.com.py/

176 Naciones Unidas. Asamblea General. (2018). Resolución A/HRC/39/29. El derecho a la privacidad en la era digital. Párr. 19. Disponible en: https://www.ohchr.org/en/documents/thematic-reports/ahrc3929-right-privacy-digital-age-report-united-nations-high: Los Gobiernos parecen recurrir cada vez más a programas informáticos de interceptación maliciosa que se infiltran en los dispositivos digitales de las personas. Este tipo de piratería informática permite la interceptación y recopilación indiscriminada de todo tipo de comunicaciones y datos, cifrados o no, así como el acceso remoto y secreto a los dispositivos personales y los datos almacenados en ellos, lo que facilita la vigilancia en tiempo real y la manipulación de los datos contenidos en esos dispositivos."

177 Naciones Unidas. Asamblea General. (2022). Resolución A/HRC/51/17. El derecho a la privacidad en la era digital. Disponible en: https://docs.un.org/es/A/HRC/51/17

A continuación se ejemplifica su utilización con casos documentados en **Paraguay, México y El Salvador.**

PARAGUAY

En el año 2012, el gobierno paraguayo adquirió el software espía *FinFisher*[178], según revelaron investigaciones del Citizen Lab de la Universidad de Toronto y el diario ABC Color. Estas investigaciones incluyen documentación oficial como facturas de compra, así como actas de entrega y recepción firmadas por la Secretaría Nacional Antidrogas (SENAD), lo que confirma el uso estatal de este malware para actividades de vigilancia.

Otro caso relevante es el del software *Galileo* – Remote Control System (RCS), desarrollado por la empresa *Hacking Team*. Las filtraciones de *Wikileaks*[179] expusieron comunicaciones entre esta empresa y el Ministerio Público de Paraguay, que evidencian una intención de compra del sistema. Posteriormente, en octubre de 2014, el socio local de *Hacking Team* solicitó un equipo adicional, lo que sugiere un interés sostenido por parte de las autoridades paraguayas en esta tecnología de espionaje.

Asimismo, las filtraciones de *Wikileaks*[180] revelaron conversaciones diplomáticas sobre la adquisición de equipos de escucha telefónica por parte del Ministerio del Interior en el año 2010. Esta práctica se concretó en 2012, durante el gobierno de Federico Franco, cuando se compró un equipo por un valor de 2,5 millones de dólares. Sin embargo, este equipo desapareció misteriosamente de las oficinas del Ministerio del Interior, según lo denunció un informe de la Auditoría General del Poder Ejecutivo en noviembre de 2013.[181]

Si bien no existen casos concretos y plenamente identificados de vigilancia a la ciudadanía en Paraguay, no se descarta que tales prácticas se estén llevando a cabo. Estos antecedentes sugieren que el país podría estar siguiendo las tendencias regionales en materia de vigilancia estatal, muchas veces marcadas por la opacidad y la falta de controles públicos.

178 Citizen Lab (2015). Pay No Attention to the Server Behind the Proxy. Disponible en https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

179 *Wikileaks*. (2014). Cable sobre Paraguay. Disponible en https://Wikileaks.org/hackingteam/emails/emailid/249367

180 *Wikileaks*. (2010). Cable sobre Paraguay Disponible en: https://Wikileaks.org/plusd/cables/10ASUNCION97_a.html

181 Sequera, M., Samaniego, M. Cibercrimen: Desafíos de la armonización de la Convención de Budapest en el Sistema Penal Paraguayo. Pág. 48. Disponible en: https://www.derechosdigitales.org/wp-content/uploads/minuta_TEDIC.pdf

MÉXICO

En México, la adquisición y abuso de tecnologías de *spyware* han sido ampliamente documentadas tanto con respecto al spyware *FinFisher* de la empresa Gamma International;[182] Galileo de *Hacking Team*;[183] como *Pegasus* de la empresa israelí *NSO Group*. A continuación, se sintetizan los principales hallazgos en cuanto al *spyware Pegasus*.[184]

NSO Group Technologies es una de las empresas cuyo nombre ha sido ampliamente vinculado a acciones de vigilancia en varios países, incluyendo México.[185] La empresa afirma que su tecnología es utilizada exclusivamente por clientes gubernamentales aprobados por el Ministerio de Defensa de Israel.[186] Pese a que afirma respetar una política de derechos humanos, el número de casos documentados en los que su tecnología se utiliza de forma abusiva contra la sociedad civil en el mundo sigue creciendo.

El primer antecedente de *Pegasus* en México se registró en 2012, cuando investigaciones periodísticas publicaron que la Secretaría de la Defensa Nacional (en adelante, "SEDENA"), se convirtió en el primer cliente internacional de *NSO Group* al adquirir el sistema *Pegasus* como parte de una serie de contratos celebrados con la empresa *Security Tracking Devices S.A. de C.V.*, los cuáles ascendieron a 5.6 mil millones de pesos.[187] Dichas contrataciones sucedieron luego de una demostración de cómo funciona el sistema *Pegasus* en mayo de 2011 al entonces presidente Felipe Calderón, así como al Secretario de Defensa Nacional, Guillermo Galván Galván.[188]

En junio de 2017, Citizen Lab, así como ARTICLE 19, la Red en Defensa de los Derechos Digitales (R3D) y SocialTIC publicaron el informe *"Gobierno Espía: Vigilancia sistemática a periodistas y defensores de derechos humanos en México"*,[189] en el cual se da cuenta de múltiples casos de intentos de infección en contra de personas defensoras de derechos humanos y periodistas con el malware *Pegasus* durante el gobierno del presidente Peña Nieto.[190]

---

182 En 2013 y 2015, una investigación de Citizen Lab –laboratorio multidisciplinario de la Universidad de Toronto–, reveló evidencia sobre la presencia de servidores de comando y control de *FinFisher* en 32 países, incluyendo en México#. El entonces Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) anunció el inicio de una investigación#, sin embargo no se informó ningún resultado relevante.

183 Una gran cantidad de correos electrónicos y documentos internos de la firma italiana *Hacking Team* fueron filtrados al público el 5 de julio de 2015. En éstos, se mostró que la empresa de software de espionaje había vendido sus productos a gobiernos de países bajo graves crisis de derechos humanos, tales como Bahréin, Sudán o Uzbekistán. De un total de 35 naciones, México resultó ser el principal cliente de la firma, con transacciones hechas por parte de diferentes gobiernos locales, dependencias y agencias federales a través de empresas intermediarias y, en prácticamente todos los casos, sin facultades legales para hacerlo. El siguiente gráfico muestra el gasto de México en relación con otros países clientes de *Hacking Team*.

184 En la región han surgido en todo caso informaciones sobre otros países donde podría haberse desplegado el uso de *Pegasus*, incluyendo posiblemente a Colombia. Sin embargo, el caso mejor documentado y sobre el que existe más abundante evidencia sobre el uso de *Pegasus* en la región es sin duda el de México.
Sobre el caso de Colombia. Disponible en: https://es.wired.com/articulos/estados-unidos-confirma-que-financio-el-uso-del-software-espia-*Pegasus*-en-colombia
Sobre El Salvador. Disponible en: https://elfaro.net/es/202503/el_salvador/27785/embajador-johnson-no-dudo-que-pudo-haberse-usado-Pegasus-en-el-salvador
Sobre Panamá. Disponible en: www.univision.com/noticias/especiales/exclusiva-martinelli-tambien-espio-a-estadounidenses-dice-testigo

185 Cox, J. & L. Franceschi Bicchierai, (2016). "Meet *NSO Group*, The New Big Player In The Government *Spyware* Business", Motherboard. Disponible en: https://motherboard.vice.com/en_us/article/nso-group-new-big-player-in-government-spyware

186 Ibidem.

187 Aristegui Noticias. (2012). Gobierno federal vía Sedena compró 5 mil mdp en equipo para espionaje. Disponible en: https://aristeguinoticias.com/1607/mexico/gobierno-federal-via-sedena-compro-5-mil-mdp-en-equipo-para-espionaje/

188 Red en Defensa de los Derechos Digitales (R3D). (2021). *NSO Group* mostró *Pegasus* a Felipe Calderón y su Secretario de Defensa. Disponible en: https://r3d.mx/2021/08/11/nso-group-mostro-Pegasus-a-felipe-calderon-y-su-secretario-de-defensa

189 Red en Defensa de los Derechos Digitales (R3D). (2017). Gobierno espía: Vigilancia sistemática a periodistas y defensores de derechos humanos en México. Disponible en: https://r3d.mx/wp-content/uploads/GOBIERNO-ESPIA-2017.pdf

190 Ahmed, A., & Perlroth, N. (2017). Using texts as lures, government *spyware* targets Mexican journalists and their families. The New York Times. Disponible en: https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html

A pesar del cambio de gobierno y de las reiteradas declaraciones del entonces presidente de la República, Andrés Manuel López Obrador, en el sentido de que ya no se vigilaría a periodistas y defensores de derechos humanos y que ya no se operaría *Pegasus* ni ningún otro sistema similar de intercepción de comunicaciones privadas, la vigilancia prevaleció en su gobierno. En 2022 y 2023, la investigación *"Ejército Espía"* reveló nuevos casos de vigilancia con *Pegasus* atribuibles con un alto grado de certeza al Ejército Mexicano.[191]

Hasta ahora, las víctimas documentadas del espionaje por parte de la SEDENA incluyen al subsecretario de Derechos Humanos, Alejandro Encinas,[192] al coordinador de la Comisión de la Verdad para la "Guerra Sucia" –el periodo de desapariciones forzadas, torturas y ejecuciones cometidas por las fuerzas de seguridad mexicanas, incluido el ejército, entre los años 1960 y 1980–, Camilo Vicente Ovalle,[193] a una organización de derechos humanos, el Centro de Derechos Humanos Miguel Agustín Pro Juárez (Centro Prodh), al defensor de los derechos humanos Raymundo Ramos, y a dos periodistas, Ricardo Raphael y un periodista del medio digital Animal Político.[194] **De hecho, las infecciones con Pegasus ocurrieron en momentos en que las víctimas realizaban labores relacionadas con violaciones a derechos humanos cometidas por las Fuerzas Armadas.**

En 2017, 2022 y 2023, las personas defensoras de derechos humanos y periodistas vigiladas por el *spyware Pegasus* presentaron denuncias penales ante la Fiscalía Especial para la Atención de Delitos Cometidos contra la Libertad de Expresión (en adelante ''FEADLE'') por, entre otros, los delitos de intervención ilegal de comunicaciones privadas y acceso ilegal a sistemas informáticos. Sin embargo, a la fecha, la impunidad ha prevalecido.

El hecho de que una de las víctimas, el Centro Prodh, haya sido objeto de vigilancia con *Pegasus* en dos administraciones distintas, y haya presentado dos denuncias penales diferentes, muestra cómo la impunidad y la falta de medidas adecuadas llevaron a la repetición de la vigilancia ilegal.

EL SALVADOR

Entre julio de 2020 y noviembre de 2021, el mismo software *Pegasus* fue utilizado para infectar 35 dispositivos pertenecientes a periodistas y miembros de la sociedad civil, según el informe del *Proyecto Torogoz* desarrollado por Citizen Lab y Access Now.[195]

El informe señaló que, de las 35 personas que fueron infectadas y vigiladas con el software, 22 personas son integrantes del medio de investigación de periodismo *El Faro*.[196] El informe además concluyó que el acceso a los dispositivos móviles de los periodistas coincide con momentos previos a la publicación de reportajes de *El Faro* con información de interés público.

---

191 Red en Defensa de los Derechos Digitales (R3D). Ejército Espía. Disponible en: https://ejercitoespia.r3d.mx/

192 Kitroeff, Natalie & R. Bergman, "Mexican President Said He Told Ally Not to Worry About Being Spied On", The New York Times, 23 de mayo de 2023, disponible en: https://www.nytimes.com/2023/05/23/world/americas/mexico-president-spying-Pegasus.html

193 Lopez, Oscar & M. Sheridan, "He's leading Mexico's probe of the Dirty War. Who's spying on him?", The Washington Post, 23 de junio de 2023, disponible en: https://www.washingtonpost.com/world/2023/06/03/mexico-Pegasus-dirty-war-lopez-obrador/

194 Red en Defensa de los Derechos Digitales (R3D), Article 19, Social Tic, et. al., Ejército Espía, disponible en: https://ejercitoespia.r3d.mx/

195 The Citizen Lab & Access Now. (2022). Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with *Pegasus Spyware*. University of Toronto. Disponible en: https://utoronto.scholaris.ca/items/025fd761-7d3f-4356-b6f8-f43eeab65128

196 Ver: https://elfaro.net/es?ref=inicio

Este caso se dió bajo el primer mandato del Presidente Nayib Bukele en El Salvador. El Gobierno negó cualquier vinculación con estos hechos y afirmó no ser cliente de *NSO Group*.[197] Sin embargo, el informe del *Proyecto Torogoz* establece que, si bien no hay pruebas que vinculen la infección concreta con un cliente de *Pegasus* en particular, se pudo identificar a un cliente de *Pegasus* que opera en El Salvador desde noviembre de 2019 al que nombraron como *"Torogoz"*.[198] Además, como fue referido con anterioridad, *NSO Group* ha declarado que este software se vende solo a gobiernos.[199]

La CIDH y su RELE, así como la Oficina Regional del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (en adelante, OACNUDH) manifestaron preocupación ante la información sobre la utilización de *Pegasus* contra periodistas y organizaciones de la sociedad civil en El Salvador. A su vez, exhortaron al Estado a investigar el caso de manera efectiva e imparcial y a velar por la protección de las víctimas.[200]

A nivel nacional, la organización *Cristosal*, dedicada a la defensa de los derechos humanos, presentó una demanda ante la Sala de lo Contencioso Administrativo de la Corte Suprema de Justicia contra la Corte de Cuentas en El Salvador por negarse a investigar el posible uso de fondos estatales para la compra de *Pegasus*. Sin embargo, la demanda fue desestimada.[201] *Cristosal* manifestó que presentarían un amparo por la falta de investigación de uso de fondos estatales para la compra del software.[202]

A nivel internacional, durante diciembre del 2022, periodistas de El Faro presentaron una denuncia contra *NSO Group* ante un Tribunal Federal en Estados Unidos. La demanda fue presentada con el objeto de que la empresa revele quién es el cliente que compró *Pegasus*, aclare qué información se recolectó de los periodistas, qué se hizo con esta información y que se elimine de sus servidores.[203] El caso fue desestimado basado en el argumento que ni los demandados ni los demandantes se encontraban en Estados Unidos.[204]

Durante julio de 2024, empresas de tecnología y organizaciones de prensa en Estados Unidos presentaron *amicus curiae* al Noveno Tribunal de Apelaciones para apoyar la demanda de los miembros de El Faro en su demanda contra *NSO Group*. La demanda se encuentra en estado de apelación por la inicial desestimación del caso.[205]

---

197 Abi-Habib, M. (2022). El software espía *Pegasus* fue utilizado para hackear a periodistas en El Salvador. The New York Times. Disponible en: https://www.nytimes.com/es/2022/01/12/espanol/el-faro-Pegasus.html

198 The Citizen Lab & Access Now. (2022). Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with *Pegasus Spyware*. University of Toronto. Disponible en: https://utoronto.scholaris.ca/items/025fd761-7d3f-4356-b6f8-f43eeab65128

199 NDTV. (2021). Firms like NSO can't sell *Pegasus* to non-government actors, Israel's ambassador to India says. Disponible en: https://www.ndtv.com/india-news/firms-like-nso-cant-sell-*Pegasus*-to-non-government-actors-israels-ambassador-to-india-2590792

200 Comisión Interamericana de Derechos Humanos (CIDH). (2022). La CIDH, su Relatoría Especial para la Libertad de Expresión y la OACNUDH expresan preocupación ante los hallazgos sobre el uso del software *Pegasus* en El Salvador. https://www.oas.org/es/cidh/jsForm/?File=/es/cidh/prensa/comunicados/2022/022.asp

201 Swissinfo.ch. (2023). El Supremo salvadoreño no admite demanda contra ente que no investigó *Pegasus*. Disponible en: https://www.swissinfo.ch/spa/el-supremo-salvadore%C3%B1o-no-admite-demanda-contra-ente-que-no-investig%C3%B3-Pegasus/48445076

202 DW. (2023, mayo 1). ONG presentará demanda de amparo ante Corte Suprema de El Salvador por espionaje con *Pegasus* a periodistas. LatAm Journalism Review. https://latamjournalismreview.org/es/news/ong-presentara-demanda-de-amparo-ante-corte-suprema-de-el-salvador-por-espionaje-con-Pegasus-a-periodistas/

203 De Assis, C. (2022). Tras haber sido espiados, algunos periodistas de El Faro demandan en Estados Unidos al fabricante del *spyware Pegasus*. LatAm Journalism Review. Disponible en: https://latamjournalismreview.org/es/articles/tras-haber-sido-espiados-periodistas-de-el-faro-demandan-en-estados-unidos-al-fabricante-del-spyware-Pegasus/

204 Electronic Privacy Information Center. (2024). Dada et al. v. *NSO Group*. Disponible en: https://epic.org/documents/dada-et-al-v-nso-group/

205 Gressier, R. (2024). Gigantes de tecnología y prensa dan espaldarazo a la apelación de El Faro en caso *Pegasus*. El Faro. Disponible en: https://elfaro.net/es/202407/el_salvador/27511/Gigantes-de-tecnolog%C3%ADa-y-prensa-dan-espaldarazo-a-la-apelaci%C3%B3n-de-El-Faro-en-caso-Pegasus.htm

V. Geolocalización basada en la explotación de vulnerabilidades en la infraestructura de telecomunicaciones (SS7)

Además de contar con antenas, la red de telefonía móvil está formada por conmutadores, interfaces y bases de datos que permiten ubicar a los dispositivos y conocer la información necesaria para proveerles el servicio de telecomunicaciones.

La forma en que nuestros dispositivos y las antenas se comunican está dictado por un protocolo. El sistema de señalización por canal común N.º 7 (SS7) es un conjunto de protocolos utilizados por los operadores de redes móviles para intercambiar información, establecer y enrutar llamadas telefónicas, mensajes de texto y otras comunicaciones dentro de las redes 2G y 3G.[206]

El protocolo fue adoptado hace casi cuarenta años, en un momento en el que el campo de telecomunicaciones móviles estaba compuesto por pocas empresas, conocidas entre sí, por lo que no fue ideado con medidas de autenticación. La falta de medidas contra accesos ilegítimos ha provocado que el protocolo sea abusado por diversas entidades para fines de vigilancia. Dos casos representativos de geolocalización con base en la explotación de dichas vulnerabilidades se encuentran en **Brasil** y **Perú**.

BRASIL

A principios de 2023, la prensa reveló que la Agencia Brasileña de Inteligencia (Abin) utilizó ilegalmente herramientas de geolocalización de dispositivos electrónicos durante el gobierno de Bolsonaro (2019-2022), siendo la principal de ellas el *spyware FirstMile*.[207]

FirstMile, desarrollado por la empresa israelí Cognyte (ex-Verint), es un software espía que explota vulnerabilidades en las redes de telecomunicaciones (SS7) para rastrear la ubicación de dispositivos móviles. La tecnología permitía monitorear hasta 10.000 teléfonos móviles por año, bastando con ingresar el número de teléfono del objetivo, independientemente de la red utilizada (3G, 4G o 5G). A partir de un número de teléfono introducido, First Mile puede proporcionar la localización de un dispositivo – y, por tanto, de la persona a la que pertenece – en función de su posición al conectarse a una red móvil.

En Brasil, la empresa *Suntech* actuó como representante y desarrolladora de *FirstMile*, según información de la Associação Catarinense de Empresas de Tecnología (Acate).[208] El contrato para la adquisición de este software fue firmado directamente por la Abin en diciembre de 2018, durante el final del gobierno de Michel Temer. La adquisición se produjo a través del contrato 567/2018[209], que es confidencial.

206 Electronic Frontier Foundation. (2024). EFF to FCC: SS7 is Vulnerable, and Telecoms Must Acknowledge That. Disponible en: https://www.eff.org/deeplinks/2024/07/eff-fcc-ss7-vulnerable-and-telecoms-must-acknowledge

207 Dantas, D.; Camporez, P.; Bronzatto, T.. Abin de Bolsonaro usou programa secreto para monitorar localização de pessoas por meio do celular. OGlobo, 14 mar. 2023. Disponible en: https://oglobo.globo.com/politica/noticia/2023/03/abin-de-bolsonaro-usou-programa-secreto-para-monitorar-localizacao-de-pessoas-por-meio-do-celular.ghtml.

208 G1. First Mile: o que se sabe sobre o software espião usado pela Abin. G1, 25 ene. 2024. Disponivle en: https://g1.globo.com/tecnologia/noticia/2024/01/25/fist-mile-o-que-se-sabe-sobre-o-software-espiao-usado-pela-abin.ghtml.

209 Ibidem.

No se sabe con certeza cuántas veces se utilizó el programa de espionaje, pero sí se tiene constancia[210] de que fue empleado para espiar a ciudadanos brasileños entre el 26 de diciembre de 2018 y el 8 de mayo de 2021, período del contrato en el que se adquirió la herramienta, según lo confirmado por la Agencia Brasileña de Inteligencia. Investigadores indican[211] que, aunque el contrato finalizó en 2021, hay señales de que el sistema fue utilizado con mayor frecuencia en los últimos años del gobierno de Bolsonaro (2019-2022) para vigilar ilegalmente a funcionarios públicos, políticos, policías, abogados, periodistas e incluso jueces y miembros del Supremo Tribunal Federal (en adelante, STF).

Por ejemplo, informes indican que el software fue ampliamente utilizado entre mayo de 2020 y abril de 2022, período en el que Alexandre Ramagem estuvo al frente de la Abin, para monitorear ilegalmente a agentes públicos –incluidos periodistas, jueces del STF y opositores políticos– y otros ciudadanos, lo que sugiere un posible uso para intimidación o control de disidencia.[212] En ese momento, la agencia operaba bajo la supervisión del Gabinete de Seguridad Institucional (GSI) de la Presidencia de la República, comandado por el general Augusto Heleno.

Las investigaciones de la Policía Federal iniciadas en 2023 sugieren que un grupo dentro de la Abin, especialmente durante la gestión de Ramagem, instrumentalizó la agencia para el monitoreo ilegal de autoridades, funcionarios públicos y otros ciudadanos sin ningún tipo de control judicial o legislativo, lo que permitió que esta vigilancia masiva ocurriera sin que las víctimas fueran notificadas o tuvieran posibilidad de defensa.[213] Su forma de utilización plantea cuestiones sobre abuso de poder y violación de derechos constitucionales.

Las investigaciones están en curso, y los documentos obtenidos hasta el momento indican que la Abin realizó operaciones ilegales de monitoreo con la herramienta durante al menos tres años, sin transparencia sobre su uso ni mecanismos de rendición de cuentas.[214] La falta de transparencia en la adquisición y el uso de la herramienta sigue siendo uno de los principales puntos de investigación por parte de la Policía Federal y el STF en 2024.

En enero de 2023, la Policía Federal lanzó la *"Operação Última Milha"* para investigar la instrumentalización de la Abin con fines políticos, la llamada "Abin paralela". Según la decisión del ministro Alexandre de Moraes, la investigación indica la existencia de un núcleo político en la Abin, especialmente bajo la gestión de Alexandre Ramagem, que utilizó tecnología de manera ilegal para monitorear a autoridades, funcionarios públicos y ciudadanos.

En enero de 2024, la Policía Federal lanzó la *Operación Vigilancia Aproximada* –ramificación de Última Milha– para investigar una organización criminal dentro de la Abin que habría monitoreado ilegalmente a personas y autoridades, invadiendo dispositivos electrónicos e infraestructuras de telecomunicaciones. Uno de los investigados es el diputado Alexandre Ramagem (PL-RJ), exdirector de la Abin. Se ejecutaron 21 órdenes de registro e incautación, y al menos siete agentes de la Policía Federal están bajo investigación. En 2025, los avances en el caso llevaron a la suspensión del policía federal Carlos Afonso Gonçalves Gomes Coelho, coordinador del Comando de Aviación Operacional de la Policía Federal, acusado de integrar el "núcleo de alta gestión" de la "Abin paralela" junto con Ramagem en la época de los hechos.

---

210 Ibidem.

211 G1. PF prende dois servidores e apura se Abin rastreou celulares de forma ilegal na gestão Bolsonaro. G1, 20 oct. 2023. Disponible en: https://g1.globo.com/politica/noticia/2023/10/20/policia-federal-abin-geolocalizacao.ghtml.

212 G1. First Mile: o que se sabe sobre o software espião usado pela Abin. G1, 25 ene. 2024. Disponivle en: https://g1.globo.com/tecnologia/noticia/2024/01/25/fist-mile-o-que-se-sabe-sobre-o-software-espiao-usado-pela-abin.ghtml.

213 Pontes. F.. Abin espionou autoridades do Judiciário, do Legislativo e jornalistas. Agência Brasil, 11 jul. 2024, disponible en: https://agenciabrasil.ebc.com.br/geral/noticia/2024-07/abin-espionou-autoridades-do-judiciario-do-legislativo-e-jornalistas.

214 Ibidem.

En enero de 2024, la Agencia Nacional de Telecomunicaciones (en adelante, Anatel) abrió tres procesos administrativos confidenciales para investigar el posible involucramiento de empresas de telefonía móvil en el monitoreo ilegal de celulares mediante el software *FirstMile*. Se investiga si las operadoras identificaron intentos de acceso indebido a la información en la época o solo tuvieron conocimiento después, a través de la prensa. También se examina su deber de comunicación a la agencia. Las empresas negaron haber tenido contacto con la Abin o conocimiento de la vigilancia ilegal, afirmando que implementaron bloqueos contra accesos indebidos mediante protocolos de interconexión internacional. Existen informes de que la Abin operó sin interacción previa con las operadoras, pero no está claro cuándo detectaron los ataques.[215]

En diciembre de 2023, la Procuraduría General de la República (en adelante, "PGR") presentó una Acción Directa de Inconstitucionalidad por Omisión (ADO 84), convertida en la Acción de Incumplimiento de Precepto Fundamental (ADPF) 1143 ante el STF. La acción cuestiona la falta de regulación sobre el uso de programas espía por organismos públicos. La PGR argumentó que la adquisición y uso sin reglas claras comprometen derechos fundamentales como la vida privada, la intimidad y el secreto de las comunicaciones. Solicitó que el Congreso establezca un plazo para aprobar una legislación sobre el tema. El caso sigue en juicio, pero en junio de 2024, el ministro Cristiano Zanin convocó una audiencia pública sobre la ADPF 1143, con la participación de 33 entidades.

PERÚ

El *Proyecto Pisco* fue una medida de vigilancia masiva implementada por el gobierno de Ollanta Humala durante los años 2011 al 2016, a través de la Dirección Nacional de Inteligencia (en adelante "DINI"). Consistió en la adquisición, sin licitación pública, de un sistema de interceptación legal de comunicaciones a la empresa israelí-estadounidense *Verint Systems*, por un valor de USD 22 millones, con financiamiento del Ministerio de Economía y Finanzas.[216]

El sistema permitía la intervención de llamadas telefónicas, mensajes de texto, correos electrónicos, chats y navegación web, así como la geolocalización en tiempo real de hasta 5,000 personas y la grabación simultánea de 300 conversaciones.[217]

Además, incluyó el módulo *SkyLock*, una herramienta capaz de localizar dispositivos móviles dentro y fuera del país.[218] Aunque fue gestionado inicialmente por la DINI, el sistema fue luego transferido al Ministerio del Interior, quedando bajo responsabilidad de la Dirección General de Inteligencia del mismo (en adelante, "DIGIMIN"). Se conoció también que las empresas operadoras Movistar, Claro, Entel y Bitel firmaron convenios de colaboración para permitir el acceso a sus redes por parte del Estado.[219]

---

215 STF: Control de constitucionalidad sobre *spyware*: [No investiga el caso concreto, sino que busca la regulación de esta tecnología.]

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

217 Associated Press (2016). Snapping up cheap spy tools, nations 'monitoring everyone'. Disponible en: https://apnews.com/736dd5c3aa644cd499d6f6da8b9e5974

218 Esta herramienta aprovecha vulnerabilidades en la infraestructura de telecomunicaciones (como SS7).

219 Derechos Digitales (2016). Perú pagó USD $22 millones para espiar las comunicaciones de sus ciudadanos. Disponible en: https://www.derechosdigitales.org/10389/peru-pago-usd-22-millones-para-espiar-las-comunicaciones-de-sus-ciudadanos/.

Durante el gobierno del expresidente Humala, hubo denuncias de seguimientos y vigilancia realizados sobre altos perfiles políticos, como el expresidente Alan García o la candidata de oposición Keiko Fujimori.[220] En consecuencia, aunque no hay víctimas identificadas públicamente ni cifras oficiales sobre personas afectadas, el diseño y alcance del sistema permite inferir que, de haberse empleado, cualquier persona con acceso a medios de comunicación digitales o telefonía móvil podría haber sido objeto de vigilancia, sin distinción de profesión o actividad.

Proyecto Pisco ha sido objeto de investigaciones legales, políticas y administrativas por diversas entidades del Estado peruano. Por ejemplo, en el ámbito penal, en el año 2023, el Ministerio Público, a través de la Fiscalía Anticorrupción, inició una investigación preliminar contra el expresidente Humala y altos exfuncionarios de su gestión por el presunto delito de colusión agravada.

En este sentido, la Fiscalía sostiene que la compra del sistema a la empresa israelí-estadounidense *Verint Systems*, valorada en USD 22 millones y realizada sin licitación pública, habría sido direccionada de manera irregular, generando un perjuicio económico al Estado. En octubre de dicho año, la Fiscalía presentó acusación solicitando 10 años y cuatro meses de prisión efectiva.[221] A la fecha, aún no se ha emitido sentencia.

En el ámbito parlamentario, en agosto de 2015, la Comisión de Inteligencia del Congreso de la República anunció que analizaría la compra del sistema, calificándola como un tema prioritario. Se programaron sesiones para evaluar el caso y se citó al entonces contralor general Fuad Khoury para rendir cuentas sobre los hallazgos de la Contraloría General de la República.

La Contraloría, por su parte, también habría iniciado investigaciones sobre la compra del sistema, aunque los resultados de estos procesos no han sido plenamente difundidos ni transparentados públicamente.

De igual forma, existen otros países, como **Paraguay**, en donde desde el 2014 el Ministerio del Interior del gobierno de Horacio Cartes cuenta con la tecnología Septler.[222] Sin embargo, por cuestiones de "seguridad", no hay detalles en el portal de contrataciones públicas y sólo se cuenta con información de la licitación a la empresa GALCORP, S.A.[223]

Por su parte, en **México** también se ha documentado el uso de geolocalización ilegal mediante la herramienta de *Geomatrix* de la empresa *Rayzone Group*, con evidencia de que la Fiscalía General de la República adquirió y operó ilegalmente el sistema de geolocalización para espiar las campañas de los candidatos presidenciales en 2018.[224]

---

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

221 Infobae (2023). Fiscalía pide diez años de cárcel contra Ollanta Humala por caso *Proyecto Pisco*. Disponible en: https://www.infobae.com/peru/2023/10/12/ollanta-humala-fiscalia-pide-diez-anos-de-carcel-por-caso-proyecto-pisco/

222 Septier. Ver: https://www.septier.com/products/

223 Contrato de licitación, disponible aquí: https://www.contrataciones.gov.py/licitaciones/adjudicacion/contrato/284615-galcorp-sociedad-anonima-1.html

224 Red en Defensa de los Derechos Digitales (R3D). (2021). #FiscalíaEspía: la FGR adquirió equipo capaz de espiar ilegalmente a todos los usuarios de Internet en México. https://r3d.mx/2021/04/14/fiscaliaespia-la-fgr-adquirio-equipo-capaz-de-espiar-ilegalmente-a-todos-los-usuarios-de-internet-en-mexico/

VI. Ciberpatrullaje

Otra de las técnicas de vigilancia identificadas en la región es el monitoreo de internet de forma masiva e indiscriminada –también conocido como "ciberpatrullaje" – y realizado, en su mayoría, por fuerzas de seguridad e inteligencia. Esta técnica consiste en el monitoreo sistemático de los contenidos que circulan en internet que, al ser considerados por las autoridades como "datos públicos" –dada su publicación y circulación en línea– se habilita su uso para cualquier fin, incluidos los de vigilancia y posterior persecución penal.[225]

El "ciberpatrullaje" puede ser desplegado tanto por las fuerzas de policía como las fuerzas militares y se intenta justificar en la prevención, detección o investigación de conductas ilícitas. Sin embargo, al realizarse de forma masiva e indiscriminada, puede derivar en afectación de derechos fundamentales como la privacidad, la protección de datos personales, la libertad de expresión y asociación y la presunción de inocencia.

En la región, Derechos Digitales recopiló en un informe de 2024[226] el despliegue de casos de ciberpatrullaje en países como Argentina, Brasil, Bolivia, Colombia, México y Uruguay, así como la adquisición de tecnologías para dicho propósito. También documentó la creación de perfiles de falsos agentes encubiertos que potencian el alcance del ciberpatrullaje en la región.

En esta sección enfocamos la atención en la experiencia de Colombia, reconociendo al tiempo que por tratarse de una práctica de vigilancia más bien nueva la documentación de información sobre su despliegue se va actualizando de manera constante.

COLOMBIA

En 2021, se llevaron a cabo diversas manifestaciones públicas en contra de la administración del Presidente Iván Duque[227], las cuales eventualmente se denominaron como el Paro Nacional de 2021. En este contexto, las redes sociales constituyeron la herramienta para denunciar abusos y violaciones de derechos humanos hacia la ciudadanía por parte de la fuerza pública.

En este periodo, el Puesto de Mando Unificado-Ciber (PMU-Ciber) realizó un monitoreo de fuentes abiertas.[228] Según las autoridades, esto buscaba la identificación de noticias falsas en las redes sociales que actuaban en contra de la imagen de las instituciones públicas y la identificación de responsables de "actos de vandalismo".

En el marco de las movilizaciones, el PMU-Ciber dedicó más de 20 mil horas en monitorear la actividad de la ciudadanía en internet, mientras adelantó una estrategia de manera simultánea para fingir un ciberataque al Ministerio de Defensa e impulsar la campaña #ColombiaEsMiVerdad.[229]

---

225 Camacho, L.; Ospina, D.; Upegui, J.C.(2022). Inteligencia estatal en internet y redes sociales: el caso colombiano. Dejusticia. Disponible en: https://www.dejusticia.org/wp-content/uploads/2022/12/InteligenciaEstatalEnInternet-Web-Dic23.pdf ; ver también: Zara, N. (2023). Inteligencia basada en fuentes abiertas (OSINT) y derechos humanos en Latinoamérica: un estudio comparativo en Argentina, Brasil, Colombia, México y Uruguay. CELE. Disponible en: https://www.palermo.edu/Archivos_content/2023/cele/papers/233008-reporte-regional-OSINT.pdf

226 Derechos Digitales (2024). Perfilamiento en redes sociales y ciberpatrullaje como nuevas modalidades de la vigilancia masiva desplegada por los Estados: casos relevantes en América Latina. Disponible en: https://www.derechosdigitales.org/wp-content/uploads/Informe-RELE-vigilancia-masiva_cerrado.pdf

227 Ivan Duque fue elegido como candidato del partido Centro Democrático, una organización política que determina como principios rectores de su móvil político "la seguridad democrática, la confianza inversionista, la cohesión social, la austeridad estatal y el diálogo popular" y que, de acuerdo a Fundación Karisma, es simpatizante con las facciones más conservadoras del campo político colombiano.

228 El PMU-Ciber consistió en la cooperación de diferentes autoridades que se coordinaron para llevar a cabo actividades de "ciberpatrullaje". Las entidades miembros del PMU-Ciber fueron, a saber, el Centro Cibernético Policial; el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC); el Grupo de respuesta a emergencias cibernéticas de MinTIC; la Dirección Nacional de Inteligencia (DNI); el Equipo de Respuesta de Incidentes de Seguridad Informática de la Policía Nacional; el Comando Conjunto Cibernético de las Fuerza Militares; y la Fiscalía General de la Nación (FGN), encabezado por Francisco Barbosa.

229 Fundación para la Libertad de Prensa (FLIP). (2021). Los jueces de la verdad, el mar de mentiras detrás del ciberpatrullaje del Estado. https://flip.org.co/pronunciamientos/los-jueces-de-la-verdad-el-mar-de-mentiras-detras-del-ciberpatrullaje-del-estado

Mediante dicha campaña se compartieron las publicaciones consideradas como falsas bajo juicio de las autoridades encargadas del monitoreo, sin explicitar bajo qué criterios una noticia era calificada como tal y sin ningún tipo de contrapeso o control. En el marco del monitoreo de redes sociales, las autoridades empezaron a denominar como "terrorismo digital" a las publicaciones identificadas como noticias falsas. La etiqueta de "terrorismo digital" estigmazó opiniones en contra de las autoridades y censuró a las personas mediante la eliminación de publicaciones y cuentas de redes sociales, en completa vulneración de los derechos al acceso a la información y la libertad de expresión.

En su momento, el Ministro de Defensa, Diego Molano, afirmó que las noticias se identificaron como falsas gracias a herramientas como *Colombiacheck* y el Detector de Mentiras de La Silla Vacía, ambos chequeadores de noticias a nivel nacional.[230] Estos dos chequeadores afirmaron que sus clasificaciones de contenidos falsos siguen determinados criterios y metodologías de chequeo, que implican la explicación del por qué se califica de esa manera y los insumos informativos.

Según una investigación realizada por *Fundación Karisma*, dentro de las actividades del ciberpatrullaje en el Paro Nacional de 2021, también se implementó la práctica del "agente encubierto en medio virtuales", de acuerdo con lo dispuesto por el art. 16 de la ley 1908 de 2018. Esto implicó el monitoreo de perfiles públicos de redes sociales y grupos de WhatsApp por parte de la Fiscalía General de la Nación, con el fin de recolectar información que sirviera de evidencia digital en los procesos posteriores de investigación para la judicialización por hechos relacionados con la protesta social en 2019 y 2021.[231]

De acuerdo con el reporte del Estado a la CIDH, con motivo de su visita de trabajo a Colombia en junio de 2021, hubo 21.675 horas de "ciberpatrullaje" desde el inicio de las manifestaciones el 28 de abril hasta el 8 de junio de 2021, siendo esta última la fecha de inicio de la visita.[232] En este periodo, las autoridades colombianas identificaron al menos 154 noticias falsas y más de 2,300 publicaciones que contenían amenazas a la vida o la integridad física.[233]

Por lo que, de acuerdo con el informe de junio de la CIDH, el ciberpatrullaje constituye un riesgo a las libertades individuales, puesto que: (a) "criminali[za] expresiones sobre funcionarios o asuntos de interés público", a la vez que (b) tiene un "fuerte efecto inhibitorio de la difusión de ideas, críticas e información".[234] La CIDH también identificó el vínculo entre el Ministerio de Defensa y la empresa Alotrópico S.A.S, relacionadas con la campaña #ColombiaEsMiVerdad, mediante un *"servicio para posicionar la "marca" del Ministerio de Defensa haciendo uso de herramientas de OSINT para actividades con marketing como los son análisis de percepción, detectar crisis de imagen en las redes sociales, identificar actores importantes o aliados en esta estrategia de comunicación"*.[235]

---

230 Saavedra, A. M. (2021, 8 de noviembre). Colombiacheck y la campaña Colombia es mi verdad. Colombiacheck. https://colombiacheck.com/investigaciones/colombiacheck-y-la-campana-colombia-es-mi-verdad

231 Fundación Karisma está próxima a publicar el informe referenciado en este apartado.

232 CIDH. (2021). CIDH culmina visita de trabajo a Colombia y presenta sus observaciones y recomendaciones. https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/prensa/comunicados/2021/167.asp

233 Los reportes sobre las acciones monitoreadas por el PMU-Ciber fueron compartidos desde el 22 de mayo de 2021 hasta el 2 de julio de 2021, mediante la cuenta de X del Ministerio de Defensa (@mindefensa). Antecedidos por otras publicaciones sobre la actividad del PMU-Ciber en enero de 2020 y en los primeros días de mayo de 2021. Así mismo, el Centro Cibernético Policial (CCP) publicó en junio del 2021 un balance general sobre la manifestación pública entre el 28 de abril y el 3 de junio de 2021. De acuerdo con esta institución, durante este periodo se identificaron "93 noticias falsas (..) que iban en contra [de] la imagen institucional, [a través de actividades de ciberpatrullaje en redes sociales]". Este reporte fue compartido también mediante su cuenta de X (@CaiVirtual). El 2 de julio de 2021 se publicó el último informe por MinDefensa en su cuenta de X, en donde señalaron haber identificado 157 noticias falsas; es decir, 3 adicionales a las reportadas ante la CIDH.

234 Comisión Interamericana de Derechos Humanos (CIDH). (2021, 10 de junio). CIDH culmina visita de trabajo a Colombia y presenta sus observaciones y recomendaciones. https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/prensa/comunicados/2021/167.asp

235 Antes del Paro Nacional de 2021, 4 entidades estatales habían contratado servicios de tecnología con empresas proveedoras de herramientas para la vigilancia digital. A saber, DIJIN; el Comando Conjunto Cibernético de la Policía; el Ejército Nacional, la Policía Nacional; y FGN. Estos contratos fueron firmados con tres empresas privadas: a. Gamma Ingenieros SAS: GAMMA Ingenieros, era distribuidor de 4IQ, una empresa española, ahora llamada Constella Intelligence que provee herramientas de inteligencia basadas en búsqueda en fuentes abiertas. La contratación realizada en 2016 fue de tipo directa entre el Ejército Nacional y la firma, y el objeto del contrato fue la adquisición de equipo de inteligencia con ampliación de licencia y arquitectura de hardware para el sistema de fuentes abiertas. El número de proceso de contratación es 325-DI-ADQ-CADCO-CENACINTELIGENCIA-2016. https://gammaingenieros.com/ b. Deinteko SAS: Representante en Colombia de la empresa isrelí, Cibersixgill (antes Sixgill). Esta empresa fue contratada por tres de las entidades señaladas anteriormente: (a) la DIJIN en 2019; (b) el Comando Conjunto Cibernético en 2020; y (c) la Fiscalía General de la Nación en 2022.

En el marco de las movilizaciones, la Fiscalía General de la Nación (FGN) estableció la Directiva 002 de 2021, mediante la cual se permitió a la FGN realizar investigaciones a hechos cometidos en protesta y judicializar mediante la aplicación del delito de terrorismo.[236] Lo anterior es bastante alarmante, porque la Directiva 002 de 2021 implicó un cambio en "la política criminal (...) que permitió las macro imputaciones, entendidas como imputaciones por delitos graves sobre hechos de menor lesividad".

Al establecer la posibilidad de aplicar el delito de terrorismo en investigaciones relacionadas con el Paro Nacional, las investigaciones podían alinearse con la narrativa sobre el "ciberterrorismo" y las implicaciones que ello traía a las judicializaciones posteriores. Además, el Estado se valió de algunas facultades establecidas en la Ley 1908 de 2018 para recolectar información, obtenida de grupos de WhatsApp o páginas públicas de redes sociales, como evidencia digital para investigaciones futuras relacionadas con el delito de terrorismo, el cual en años anteriores no se podía considerar como aplicable en contextos de protestas (Directiva 0008 de 2016).

De acuerdo con la investigación de Fundación Karisma, posterior a las manifestaciones de 2021, por información brindada por la FGN, se identificaron al menos 538 personas vinculadas a hechos ocurridos en el marco de la protesta entre abril y julio de 2021. 259 de ellas están imputadas en diferentes ciudades de Colombia (Bogotá, Cali, Medellín, Pasto y Bucaramanga). Según la información recolectada, la FGN recolectó información durante el periodo de análisis y ha hecho uso de la misma como evidencia digital para llevar a cabo condenas por los delitos de concierto para delinquir, terrorismo, violencia contra servidor público, daño en bien ajeno agravado y obstrucción a vías públicas que afecten el orden público.

A la fecha, no se ha iniciado ninguna investigación por potenciales abusos en el uso de las capacidades del PMU-Ciber. La única acción relacionada se dió por la nueva Fiscal General, Adriana Camargo, misma que emitió una nueva Directiva 0001 de 2024,[237] por la que deroga lineamientos establecidos en la Directiva 0002 de 2021 y establece que la protesta social pacífica goza de protección constitucional,[238] por lo que no será objeto de persecución o sanción penal. Además, establece criterios nuevos para la interpretación de actos con característica de delito sucedidos en protesta. A diferencia de la Directiva 0002 de 2021, los parámetros de interpretación para evaluar casos de investigación por terrorismo siguen una lógica de no criminalización de la protesta.

236 Ver: https://cr00.epimg.net/descargables/2021/06/06/8e14ef349816167a499eadd80bbfe740.pdf

237 Ver: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=166137

238 La Directiva determina que este tipo de actos "deben interpretarse conforme al ámbito de protección de los derechos fundamentales de libertad de expresión, libertad de reunión y manifestación pacífica y, solo aquellos que excedan el ejercicio legítimo de estos derechos, se investigarán y judicializarán de acuerdo con las reglas sustanciales y procesales penales".

VII. Vigilancia de personas a través de sistemas de lectura de matrículas de automóviles

Los lectores automáticos de matrículas son sistemas de cámaras de alta velocidad controlados por ordenadores, instalados en postes, vehículos policiales, farolas u otras estructuras, para registrar de manera automática las matrículas de los vehículos, ubicación, la fecha y la hora en que fueron captadas.[239]

Esta medida de vigilancia permite el registro, almacenamiento y análisis sistemático de matrículas de automóviles que circulan en espacios públicos de forma masiva e indiscriminada. Tiene por objeto supuesto fines de seguridad o gestión del tráfico. Sin embargo, su aplicación puede incurrir en afectaciones a derechos fundamentales como el derecho a la privacidad, circulación y protección de datos.

BRASIL

La Plataforma Integrada de Operaciones y Monitoreo de Seguridad Pública (*Córtex*) es una iniciativa del Ministerio de Justicia y Seguridad Pública (en adelante, "MJSP") de Brasil, establecida oficialmente mediante la Portaria nº 218, de 29 de septiembre de 2021. Esta plataforma es operada y gestionada directamente por la Secretaría de Operaciones Integradas (en adelante, ''SEOPI'') del mencionado ministerio.

Cortex se vincula con el programa *Smart Sampa*, iniciativa de la Prefeitura de São Paulo que integra cámaras de vigilancia en la ciudad para *presuntamente* mejorar la seguridad pública. No se han encontrado detalles públicos sobre la participación de desarrolladores o intermediarios privados específicos en la implementación o gestión de la plataforma *Córtex* o del programa *Smart Sampa*.

Su despliegue se llevó a cabo principalmente durante el gobierno de Jair Bolsonaro (2019-2022), aunque su uso continúa bajo la administración de Luiz Inácio Lula da Silva (2023-presente). Durante el gobierno de Bolsonaro, el MJSP, a través de la SEOPI, fue responsable de la gestión y operación del *Córtex*.[240]

Informes señalan que, durante el gobierno de Jair Bolsonaro, el Ministerio de Justicia optó por no auditar el sistema *Córtex*, lo que ha generado debates sobre posibles usos indebidos de la plataforma para monitorear objetivos sin justificación adecuada.[241]

En un artículo de 2020,[242] The Intercept definía Cortex como una:

> tecnología de inteligencia artificial que utiliza la lectura de matrículas por miles de cámaras de carretera repartidas por autopistas, puentes, túneles, calles y avenidas de todo el país para rastrear objetivos móviles en tiempo real.

---

239 EFF. (s.f.). Lectores automatizados de matrículas (ALPR). Disponible en: https://sls.eff.org/es/technologies/lectores-automatizados-de-matriculas-alpr

240 La Seopi es un sector del MJSP que ganó notoriedad en julio de 2020, cuando salió a la luz la existencia de un dossier de inteligencia producido por la secretaría contra policías y profesores vinculados a movimientos antifascistas, el cual fue suspendido por el STF tras un juicio. En São Paulo, la iniciativa *Smart Sampa*, promovida por la Prefeitura Municipal, busca mejorar la seguridad urbana a través de tecnologías avanzadas.

241 Freitas, C.; Valente, R.. Ministério da Justiça não quis auditar o uso do *Córtex* pelo governo Bolsonaro. Agência Pública, 12 oct. 2024. Disponible en: https://apublica.org/2024/10/cortex-mj-nao-quis-auditar-sistema-espiao-pelo-governo-bolsonaro/.

242 Rebello, A.. Da placa de carro ao CPF. The Intercept Brasil, 21 sep. 2021. Disponible en: https://www.intercept.com.br/2020/09/21/governo-vigilancia-cortex/.

Cortex es un sistema de monitoreo masivo que integra bases de datos nacionales y municipales con tecnologías de reconocimiento de placas y, en algunos casos, reconocimiento facial. No sólo monitorea en tiempo real los vehículos a través de cámaras instaladas en carreteras, identificando matrículas y rastreando sus trayectos, sino que también es capaz de recopilar y cruzar datos personales de más de 160 bases de datos –incluidas las de la administración pública federal, como el Informe Anual de Información Social del Ministerio de Economía–, conservando los datos durante un periodo de diez años.

El sistema permite que aproximadamente 55 mil agentes, civiles y militares, monitoreen "objetivos" sin la necesidad de justificaciones específicas. Según la Agencia Pública,[243] en 2024 la plataforma recibió imágenes de 35,9 mil cámaras instaladas en carreteras, zonas urbanas, estadios de fútbol y vías federales. Operando las 24 horas del día, el sistema permite la vigilancia continua de personas y vehículos.

Córtex fue objeto de una solicitud de acceso a la información en 2024,[244] por la que se buscaba conocer cuántas personas y vehículos habían sido monitoreados. El MJSP negó la respuesta, argumentando que divulgar la información podría comprometer investigaciones en curso, pero confirmó que los "objetivos" de *Córtex* pueden ser monitoreados por tiempo indefinido, hasta que surjan indicios para su imputación, debido a su función como "herramienta auxiliar de investigación". En 2022, en respuesta a una solicitud similar, reveló que hasta ese momento el sistema había identificado aproximadamente 360 mil objetivos y permitido la recaptura de más de 20 mil personas.

También hay indicios de que municipios, gobiernos estatales y otros organismos tienen acceso irrestricto al *Córtex*, siempre que ofrezcan una "contraprestación", es decir, el intercambio de sus bases de datos. Hasta marzo de 2023, el MJSP había firmado 184 Acuerdos de Cooperación Técnica (ACT) bajo este modelo.

El 10 de enero de 2025, el gobierno federal firmó un acuerdo de cooperación con São Paulo, la ciudad más populosa de Brasil, para integrar las cámaras de *Smart Sampa* –que actualmente cuenta con más de 20 mil cámaras inteligentes– con la Plataforma *Córtex*.[245] Lo cual permite que las cámaras municipales equipadas con reconocimiento de placas vehiculares accedan a la base de datos nacional sobre vehículos robados, emitiendo alertas a las autoridades correspondientes para su intervención.

Un artículo de la revista Crusoe sobre el tema indicaba que los policías pueden incluso identificar, en tiempo real, si un vehículo estaba en una playa determinada.[246] En una noticia más reciente, el mismo medio también reveló que el MJSP ha estado alimentando el *Córtex* con acceso a registros de estudiantes de las redes municipales de enseñanza.[247]

Desde su oficialización, la sociedad civil se ha movilizado contra la plataforma *Córtex*. En 2020, después de que The Intercept publicara un artículo sobre *Córtex*, la Coalición por los Derechos en Internet emitió un comunicado en el que acusaba a la plataforma de ser incompatible con los principios que rigen la protección de datos personales y un instrumento para el ejercicio del autoritarismo, algo inaceptable en un Estado democrático de derechos.[248]

---

243 Valente, R.; Freitas, C.. Programa de vigilância do MJ permite a 55 mil agentes seguir "alvos" sem justificativa. Agência Pública, 9 oct. 2024.
Disponible en: https://apublica.org/2024/10/vigilancia-55-mil-agentes-podem-monitorar-alvos-sem-justificativa/#_.

244 A través de la Agencia Pública a través de la Ley de Acceso a la Información (LAI).

245 Cidade de São Paulo. Câmeras do *Smart Sampa* começam a ler placas para identificar veículos roubados. Notícias, 10 ene. 2025. Disponible en: https://capital.sp.gov.br/w/c%C3%A2meras-do-smart-sampa-come%C3%A7am-a-ler-placas-para-identificar-ve%C3%ADculos-roubados-%C2%A0%C2%A0.

246 BIG brother federal. Crusoe. 21 ene. 2022. Disponible en: https://crusoe.com.br/edicoes/195/big-brother-federal/.

247 Valente, R.; Freitas, C.. Inteligência do Ministério da Justiça tem acesso a cadastros de alunos, revelam documentos. Agência Pública, 3 feb. 2025. Disponible en: https://apublica.org/2025/02/cortex-ministerio-da-justica-monitora-ate-dados-de-alunos-e-pais/.

248 Coalición por los Derechos en Internet. Sistema *Córtex*, do governo federal, ameaça direitos dos cidadãos. Coalición por los Derechos en Internet, 1 oct. 2020. Disponible en: https://direitosnarede.org.br/2020/10/01/sistema-cortex-do-governo-federal-ameaca-direitos-dos-cidadaos/.

En 2022, las ONG Data Privacy Brasil, Conectas, Transparencia Internacional y Artigo 19 presentaron una denuncia ante el Ministerio Público Federal argumentando que *Córtex* permitía el acceso y compartición de datos personales y sensibles sin una gobernanza efectiva, lo que habría margen para abusos y monitoreo ilegal sin rendición de cuentas.[249]

La denuncia señalaba que se trata de un "panóptico virtual" y la insuficiencia del marco normativo que regula Cortex, indicando que la Ordenanza 218/2021 no ayuda a comprender el alcance del sistema y, menos aún, a entender las salvaguardas relacionadas con su uso - indicando que, por ejemplo, la Ordenanza permite tomar decisiones ad hoc sobre quién debe ser incluido en el cerco electrónico y no estipula criterios básicos de debido proceso e investigación continua, basada en pruebas y razones legítimas de tal violación de los derechos fundamentales, para que una persona sea constantemente vigilada por el Cortex». En la denuncia, las ONG exigen información sobre el sistema, así como la apertura de una investigación civil y la realización de las diligencias necesarias para esclarecer lo expuesto. En enero de 2025, sin embargo, el MPF decidió archivar la investigación, argumentando que no se encontraron evidencias de irregularidades que justificaran la continuidad del proceso - la plataforma funcionaba dentro de un marco normativo y contaba con mecanismos internos de auditoría y control de accesos.

Artículos periodísticos alertando sobre los riesgos y la opacidad del sistema también han sido publicados por Agência Pública y plea Crusoé.[250] En 2024, una nueva carta abierta de la Coalición afirmó que "el sistema *Córtex* y su gestión actual representan una violación sistemática a la protección de datos personales".[251]

249 Ver: https://www.telesintese.com.br/wp-content/uploads/2022/02/representacao-controle-externo-da-atividade-policial.pdf.

250 Valente, R.; Freitas, C.. Programa de vigilância do MJ permite a 55 mil agentes seguir "alvos" sem justificativa. Agência Pública, 9 oct. 2024. Disponible en: https://apublica.org/2024/10/vigilancia-55-mil-agentes-podem-monitorar-alvos-sem-justificativa/#_.; y Crusoé. Big Brother Federal. Crusoé, 21 ene. 2022. Disponible en: https://crusoe.com.br/edicoes/195/big-brother-federal/.

251 Coalición por los Derechos en Internet. Posicionamento da Coalizão Direitos na Rede e entidades parceiras sobre o sistema *Córtex* do Ministério da Justiça e Segurança Pública. Coalición por los Derechos en Internet, 8 nov. 2024. Disponible en: https://direitosnarede.org.br/2024/11/08/posicionamento-cdr-entidades-parceiras-sistema-cortex-do-mj/.

En resumen

Los casos documentados en este Capítulo ilustran la preocupante tendencia al alza en el uso de tecnologías para obstaculizar la defensa de derechos humanos y el periodismo investigativo; para atacar, censurar, reprimir y perseguir a personas que revelan información de interés público (particularmente aquéllas históricamente excluidas); y para preservar la falta de rendición de cuentas en contextos latinoamericanos con una legacía de represión, impunidad y constantes violaciones de derechos humanos.

Por ejemplo, en **Chile** se reveló el monitoreo ilegal de dirigentes sociales, defensoras de derechos humanos y sindicatos por parte de Carabineros. De igual forma, la Fiscalía Metropolitana Occidente de Chile solicitó a los proveedores de servicios de internet acceso a datos personales sensibles en el marco de un estallido social y político. En **Colombia**, en lo que concierne a *ciberpatrullaje* y a raíz de las diversas manifestaciones públicas en contra de la administración del Presidente Duque, el PMU-Ciber realizó un monitoreo de redes sociales, vulnerando así los derechos de acceso a la información y libertad de expresión de millones de personas. De igual forma, FLIP documentó e identificó un total de 52 casos de periodistas vigilados de manera ilegal por el Ejército Nacional para junio de 2020 mediante un software de seguimiento informático, realizando perfilamientos ilegales a más de 130 personas.

En **México** se ha documentado tanto el acceso ilegal a datos conservados por empresas de telecomunicaciones para vigilar a personas periodistas, peritas y activistas sociales, como el uso de *spywares* contra personas periodistas y defensores de derechos humanos que denuncian actos de corrupción y violaciones de derechos humanos cometidas por el Estado, principalmente el Ejército mexicano. En la misma línea, en **El Salvador** también se documentó el uso de *Pegasus* contra periodistas y miembros de la sociedad civil. En **Paraguay**, se documentó la adquisición del software espía *FinFisher* y las filtraciones de *Wikileaks* revelaron la adquisición de equipos de escucha telefónica por el Ministerio del Interior.

Adicionalmente, la mayoría de estas medidas de vigilancia se han realizado de manera **ilegal**, pues han sido implementadas sin cumplir con los principios de legalidad, idoneidad, necesidad y proporcionalidad, así como sin contar con las salvaguardas adecuadas, reflejando abusos, falta de transparencia e impunidad. En todos los casos se identificaron vulneraciones a derechos humanos fundamentales como la privacidad, la protección de datos personales, la libertad de expresión y asociación, en contextos en los que las personas principalmente afectadas tienen perfiles en torno al ejercicio del periodismo, activismo, movimientos sociales y oposición política.

Por otra parte, los casos documentados también reflejan una tendencia estatal y regional de robustecimiento de la vigilancia masiva e indiscriminada, como lo fueron los casos identificados de intervención de comunicaciones privadas en **Colombia, Chile** y **Perú**, así como el acceso a los registros de datos conservados de la totalidad de las personas usuarias de telefonía móvil en **Paraguay, Chile** y **México**, afectando con ello distintas libertadas del grosso de la población, incluyendo nuestro derecho a la presunción de inocencia, principio de no discriminación y autodeterminación.

En esta línea, se identificaron patrones preocupantes no sólo de colaboración entre empresas de telecomunicaciones y organismos estatales en actividades de vigilancia de comunicaciones privadas, sino también de geolocalización basada en la explotación de vulnerabilidades en la infraestructura de telecomunicaciones (SS7) y de monitoreo de las redes públicas.

El caso de **Brasil** ejemplifica cómo la ABIN utilizó ilegalmente herramientas de geolocalización de dispositivos electrónicos durante el gobierno de Bolsonaro, siendo el principal *spyware FirstMile*. En **Perú**, el gobierno de Ollanta Humala implementó un sistema de vigilancia masiva que permitía la interceptación de comunicaciones y la geolocalización de miles de personas, incluso fuera del país.

El caso brasileño también ilustra la vigilancia de personas a través de sistemas de lectura de matrículas de auto que permite el registro, almacenamiento y análisis sistemático de matrículas de automóviles que circulan en espacios públicos de forma masiva en indiscriminada. Estos casos ponen de manifiesto el uso ilegal de medidas de vigilancia por parte de los Estados en colaboración con actores privados, vulnerando a su vez derechos humanos fundamentales.

Finalmente, los casos de extracción de información detectados en la región con herramientas de extracción forense como el caso de México con la adquisición de herramientas desarrolladas por **Cellebrite** y la evidencia de la utilización de **Septier** en Paraguay demuestran la falta de transparencia en el uso de estas herramientas por las autoridades estatales.

CAPÍTULO CUATRO: DIAGNÓSTICO

La evolución tecnológica ha permitido el uso de un amplio espectro de medidas de vigilancia en la región, cada vez más avanzadas e invasivas, sin una regulación que se adecue a dichos avances para que cumplan con los estándares internacionales en materia de derechos humanos previstos en el Capítulo Dos.

En esta línea, a partir de un análisis comparativo de la normativa en torno a la vigilancia de las comunicaciones, hemos identificado una recurrente deficiencia normativa en cuanto a leyes que establezcan de manera precisa, detallada y clara las autoridades, procedimientos y circunstancias en los que se podrá hacer uso de medidas de vigilancia.

I. Requisitos de procedencia material

Las circunstancias o procedimientos para poder hacer uso de medidas de vigilancia de las comunicaciones varían significativamente entre los países de la región, pero coinciden en que en la mayoría de los casos están previstos de manera amplia, ambigua y/o vaga, dejando a la ciudadanía en un estado de indefensión que fomenta la discrecionalidad y abusos en la práctica. Lo anterior se ejemplifica con deficiencias legales en Brasil, Colombia, México y Perú.

En el caso de **Brasil**, la Ley N.° 9.883/1999 crea la ABIN y tiene por objeto establecer "el Sistema Brasileño de Inteligencia, que integra las acciones de planificación y ejecución de las actividades de inteligencia del país, con la finalidad de proporcionar apoyo al Presidente de la República en asuntos de interés nacional".[252]

Las preocupaciones relacionadas con la vigilancia estatal están, en gran medida, dentro del ámbito de la Inteligencia Brasileña.[253] La ley que regula la ABIN define competencias excesivamente amplias, lo que genera preocupaciones sobre sus límites. Por ejemplo, el artículo 4 establece atribuciones genéricas, como la recopilación y análisis de datos confidenciales para asesorar al Presidente de la República; la protección de información sensible relacionada con la seguridad del Estado y la sociedad; y la evaluación de amenazas internas y externas al orden constitucional. Esta amplitud deja margen para interpretaciones extensivas, creando un escenario similar al de la antigua Ley de Seguridad Nacional,[254] que, durante la dictadura militar, fue utilizada para justificar abusos.

En **Colombia**, la Corte IDH, en ocasión del caso *Miembros de la Corporación Colectivo de abogados "José Alvear Restrepo" Vs. Colombia*, reconoció la responsabilidad del Estado en abusos de la función de inteligencia y ordenó la reforma de la Ley 1621 de 2013 –que regula las actividades de inteligencia y contrainteligencia–[255] para incluir garantías como los principios de legalidad y debido proceso, así como la necesidad de control judicial. Actualmente se presentó en el Congreso un proyecto de ley de reforma que propone cambios sustanciales a la Ley para cumplir con la sentencia de la Corte IDH.

---

252 Ver: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11693.htm#art21

253 Escola de Ativismo. (2024). Tecnoautoritarismo: o que a "Abin paralela" nos diz sobre mecanismos de vigilância e democracia? https://escoladeativismo.org.br/tecnoautoritarismo-o-que-a-abin-paralela-nos-diz-sobre-mecanismos-de-vigilancia-e-democracia/) Nota: La ABIN arrastra una herencia estructural y operativa (del Servicio Nacional de Informações (SNI) órgano de la dictadura responsable de la vigilancia y represión de militantes, activistas, partidos políticos, sindicatos, medios de comunicación y otros sectores de la sociedad. (https://oglobo.globo.com/politica/noticia/2024/02/04/quais-sao-os-limites-maior-escandalo-da-abin-reabre-discussao-sobre-as-atividades-de-inteligencia.ghtml).

254 Ibídem.

255 Incluido el monitoreo del espectro electromagnético y las interceptaciones a las comunicaciones privadas.

En cuanto a **México**, la claridad y precisión de los requisitos de procedencia material para llevar a cabo medidas de vigilancia es variable dentro del marco jurídico mexicano. Por ejemplo, el CNPP[256] establece que la procedencia de la solicitud de autorización para la intervención de comunicaciones privadas, el acceso a datos conservados o la geolocalización en tiempo real únicamente requiere que el titular del Ministerio Público "considere necesaria" la intervención dentro de una carpeta de investigación en la que se investiga la comisión de un delito.

La constatación de la necesidad de las medidas debe ser apreciada por el juez de control federal competente a partir de indicios objetivos presentados por la autoridad que solicita autorización, sin embargo, la redacción difiere en exceso a la propia autoridad para justificar la pertinencia de una medida de vigilancia.

Sobre **Perú**, el Decreto Legislativo N.º 1141 –que regula el funcionamiento de la Dirección Nacional de Inteligencia (DINI) y del Sistema Nacional de Inteligencia (SINA)–, si bien establece que las actividades de inteligencia deben desarrollarse con respeto a los derechos humanos, contempla límites muy vagos y carece de mecanismos efectivos de control y supervisión externa, lo que permite márgenes amplios para el abuso.

De igual forma, el Decreto Legislativo N.º 1182 (denominada como Ley *Stalker*), obliga a las operadoras a conservar datos masivos de tráfico y localización de todos los usuarios por tres años, sin criterios razonables de proporcionalidad o necesidad. Además, recientes reformas han ampliado los supuestos en los que la policía puede requerir estos datos, debilitando aún más las garantías judiciales y el control ciudadano.[257]

En muchos casos, la autorización para acceder a la información es concedida por un funcionario jerárquicamente superior dentro de la misma entidad que realiza la solicitud. Esta dinámica se presenta en países como Brasil (con la ABIN y la policía), México (a través de la LGN), Perú (mediante la PNP y el OSIPTEL) y Colombia (con las Fuerzas Militares, la Policía Nacional y la Dirección Nacional de Inteligencia). Esta concentración de funciones ha generado inquietudes, puesto que no existe la independencia entre quienes investigan y quienes deben autorizar tales medidas, lo que puede derivar en abusos o falta de control externo.

En consecuencia, los marcos legales deben prever una institución civil independiente de los servicios de inteligencia y del Poder Ejecutivo, con conocimientos técnicos, para poder fiscalizar y hacer rendir cuentas a las autoridades facultadas, tanto en cuanto a sus obligaciones de transparencia como en términos de rendición de cuentas.

II. Control judicial

Como fue mencionado en el primer y segundo capítulo, la autorización judicial de medidas de vigilancia es una garantía fundamental para la prevención de abusos, arbitrariedades y discrecionalidad por parte de las autoridades. Por ello, son particularmente preocupantes las legislaciones de **Paraguay** y **Perú** que no establecen el requisito de control judicial previo.

Con base en el Decreto Legislativo N.º 1182, conocido como "Ley Stalker", **Perú** autoriza en casos de presunta flagrancia delictiva a la Policía Nacional a acceder a datos de geolocalización en tiempo real sin orden judicial previa.

---

256 Artículo 291.

257 Se conoce al menos un litigio relevante vinculado a esta norma: una demanda para obtener acceso al protocolo interno de la PNP sobre cómo se solicita y procesa la geolocalización sin orden judicial. Resultado: el pedido fue negado, y el protocolo se mantiene en reserva, lo cual refleja la falta de transparencia, opacidad institucional y ausencia de control democrático sobre esta forma de vigilancia.

Por otro lado, incluso si la legislación de los países de la región establece la necesidad de un control judicial previo, se han planteado desafíos importantes con la previsión de mecanismos excepcionales como es el caso de **Brasil**, **México** y **Paraguay**.

Así, a pesar de que **Brasil** requiere de autorización judicial tanto para la obtención de metadatos como de información de geolocalización,[258] también prevé que, si el tribunal no se pronuncia en un plazo de 12 horas, el Ministerio Público o un agente de policía pueden solicitar los datos directamente a las empresas de telecomunicaciones y telemática.

De igual forma, la ABIN – principal entidad estatal autorizada para llevar a cabo actividades de vigilancia con fines de inteligencia – no tiene prerrogativa para realizar intervención de las comunicaciones sin autorización judicial. Sin embargo, puede acceder a información obtenida por otros órganos del Sisbin[259] a través de mecanismos de cooperación establecidos en la legislación vigente.

En **México**, si bien el artículo 16 constitucional establece la necesidad de contar con una autorización judicial federal para llevar a cabo la intervención de comunicaciones privadas, el mecanismo excepcional establecido en el artículo 303 del CNPP faculta a las fiscalías a solicitar el acceso a datos conservados o la geolocalización en tiempo real a empresas de telecomunicaciones sin obtener previamente una autorización judicial, sino con la carga de solicitar la ratificación de la medida dentro de las 48 horas posteriores a la solicitud original.

Esto ha provocado que la excepción se convierta en la regla general y que un número importante de solicitudes realizadas bajo el mecanismo excepcional no sean ratificadas por la autoridad judicial federal –o inclusive ni siquiera sean sometidas a dicha ratificación–, permitiendo así que autoridades invadan la privacidad de personas usuarias de telecomunicaciones ilegal e impunemente, sin que la persona afectada o un juez siquiera tengan conocimiento de ello.

En **Paraguay** si bien el artículo 200 del Código Procesal Penal establece que la intervención de las comunicaciones requiere una resolución fundada del juez, su artículo 228 otorga tanto al juez como al Ministerio Público la facultad de requerir informes a personas o entidades públicas o privadas. Estos informes pueden ser solicitados de forma verbal o escrita, especificando el procedimiento correspondiente, el nombre del imputado, el lugar de entrega, el plazo para su presentación y las consecuencias en caso de incumplimiento. De este modo, se permite el acceso a datos conservados por empresas de telecomunicaciones sin necesidad de autorización judicial.

III. Proliferación de tecnologías de vigilancia masiva

A partir de los principios de necesidad y proporcionalidad, las medidas de vigilancia únicamente pueden ser consideradas legítimas si constituyen la alternativa menos lesiva disponible para conseguir un objetivo legítimo y si, después de un ejercicio de ponderación, las afectaciones a la privacidad y la seguridad no resultan exageradas o desmedidas frente a las ventajas obtenidas la vigilancia propuesta.

La creciente proliferación de equipos y sistemas de vigilancia como las antenas falsas o el *spyware*, que además de ser operadas de manera autónoma, sin necesidad de colaboración de ente alguno y de poseer capacidades intrusivas amplias, contiene medidas para dificultar su detección, es indicativa de la poca claridad y precisión sobre los métodos de vigilancia que pueden considerarse compatibles con las normas de derechos humanos reconocidas en las constituciones de los países de la región.

---

258 De acuerdo con el artículo 10, § 1 del Marco Civil da Internet (Ley N ° 12.965/2014) y el artículo 13-B del Código de Procedimiento Penal.

259 La ABIN forma parte del Sistema Brasileiro de Inteligência (Sisbin), que integran diversos órganos de la administración pública federal responsables de producir información relevante para las actividades de inteligencia. La operación del SISBIN está regulada por la Ley nº 9.883/99 y el Decreto nº 11.693/23.

El problema se exacerba cuando no sólo existe una ausencia de regulación de estas nuevas tecnologías, sino una tendencia por parte de algunos de los países de la región por legitimar medidas de vigilancia masiva e indiscriminada que son incompatibles con los estándares internacionales en materia de derechos humanos.

Por ejemplo, en **Chile** genera preocupaciones la reciente sanción de la Ley Antiterrorismo N.º 21.732 de febrero de 2025, que habilita al uso de tecnologías como los *IMSI Catchers* y tiene como fin "determinar, registrar y monitorear" datos que permitan "singularizar o identificar uno o más dispositivos" o facilitar su geolocalización.[260]

Entre los riesgos identificados en el uso de este tipo de tecnología de vigilancia masiva, se señala cómo se trata no sólo de una tecnología de vigilancia indiscriminada, sino en extremo desproporcionada, en tanto captura la señal de todos los dispositivos cercanos a la antena falsa, impactando con ello en la privacidad de terceras personas que no están relacionadas de ninguna manera con la investigación criminal en curso, y que en cambio legítima en la práctica la así denominada *"pesca milagrosa"*.

Por su parte, en **Colombia** el artículo 15 de la Resolución 5839 de 2015 de la Policía Nacional establece las funciones del Centro Cibernético Policial, entre las que incluye, en el punto 12, la "realiza[ción] de ciberpatrullajes 24/7 en la web con el propósito de identificar amenazas desde y hacia detección de factores comunes en los incidentes de su conocimiento así como la vulneración a la disponibilidad, integridad y confidencialidad de la información que circulan por el ciber espacio."

En la misma línea, en **México**, el artículo 9, fracción XXXVII, de la Ley de la Guardia Nacional faculta a dicha institución militarizada a realizar *"acciones de vigilancia, identificación, monitoreo y rastreo en la red pública de Internet sobre sitios web, con el fin de prevenir conductas delictivas"*. La vaguedad con que se encuentra descrita dicha facultad no permite determinar con claridad el alcance de la misma. Sin embargo, podría entenderse que en dicha facultad se pretende fundamentar la investigación de fuentes abiertas y la formulación de perfiles sobre personas usuarias de Internet.

IV. Falta de transparencia y corrupción en la adquisición de tecnologías de vigilancia

A nivel global, y en la región, los procesos de contratación de equipos y sistemas para la vigilancia de comunicaciones se han distinguido por la opacidad, discrecionalidad y por la ausencia de regulación y controles adecuados para inhibir la corrupción, la vigilancia ilegal y la impunidad.

Por ejemplo, en **Paraguay**, la Fundación Parque Tecnológico de Itaipú (PTI) continúa con una polémica licitación realizada en abril de 2015 de equipos de espionaje valuados en 12 millones de dólares, denunciada por irregularidades por el diputado Mauricio Espínola.[261] Entre las empresas oferentes figuran ITTI Saeca y Technoma, ambas vinculadas al Grupo Vázquez y al presidente Santiago Peña, así como TSV SRL, firma con antecedentes de colusión y favorecida en múltiples contratos estatales[262].

260 Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=1211036

261 Ultima Hora (2025) Dos firmas ligadas a Peña, y una con antecedentes, compiten en PTI Disponible en: https://www.ultimahora.com/dos-firmas-ligadas-a-pena-y-una-con-antecedentes-compiten-en-pti

262 ABC Color (2025) Postergan apertura de sobres de ofertas en licitación de aparatos de escucha en el PTI. Disponible: https://www.abc.com.py/este/2025/04/11/postergan-apertura-de-sobres-de-ofertas-en-licitacion-de-aparatos-de-escucha-en-el-pti-en-la-que-compiten-firmas-ligadas-al-presidente-santiago-pena/

La licitación contempla una plataforma de espionaje integral que incluye tecnologías como sistemas de interceptación legal de comunicaciones *(Lawful Interception)*, captadores *IMSI Catcher* para rastreo de dispositivos móviles, kits de análisis forense digital (como *Cellebrite* o similares), software de reconocimiento facial, herramientas OSINT para monitoreo de redes sociales y fuentes abiertas, equipos de geolocalización satelital *(GPS Trackers)* y tecnología de vigilancia acústica. Según más de 130 protestas, las especificaciones técnicas de los equipos estarían diseñadas para favorecer exclusivamente a la empresa ITTI Saeca.

En **Brasil**, ante el vacío regulatorio, la Procuraduría General de la República (PGR) presentó en diciembre de 2023 la Acción Directa de Inconstitucionalidad por Omisión N.º 84 ante el Supremo Tribunal Federal (STF), convertida en la Argución de Incumplimiento de Precepto Fundamental N.º 1.143.[263]

La acción cuestiona la posible falta de legislación sobre la compra y el uso de tecnologías de espionaje y solicita al STF que: *(i)* se reconozca la omisión del Congreso en la regulación del uso de *spyware*; *(ii)* se establezca un plazo para su regulación; y *(iii)* se implementen medidas provisionales para garantizar la protección de la privacidad y el secreto de los datos. El caso aún se encuentra en proceso.

En la misma línea, en 2024 el ministro ponente Cristiano Zanin, del Supremo Tribunal Federal, convocó una audiencia pública sobre la ADPF 1.143, con la participación de 33 entidades de la sociedad civil para contribuir al debate sobre la compra y el uso de estas tecnologías de vigilancia. InternetLab, junto con Data Privacy Brasil, participaron en la audiencia pública como *amicus curiae* y presentaron sus argumentos.[264] Así mismo destacaron que la ausencia de regulación sobre estas herramientas compromete la confianza pública en las instituciones democráticas, ya que abre espacio para abusos de poder.

En **México**, a través de solicitudes de acceso a la información, periodismo investigativo y filtraciones de información, se han identificado como las principales irregularidades respecto de los procesos de contratación de equipos y sistemas para la vigilancia: (a) la discrecionalidad y adjudicación a empresas con irregularidades (en procesos de adjudicación directa con empresas sin antecedentes o experiencia en la materia); *(b)* sobreprecios en la adquisición (montos exorbitantes y condiciones irrazonables); *(c)* contrataciones que pretenden ser escondidas u ofuscadas a partir de descripciones vagas del objeto de las contrataciones; *(d)* ausencia de controles para evitar la adquisición ilegal de tecnologías de vigilancia; y *(e)* ausencia de documentación sobre la adquisición y uso de equipos y sistemas de vigilancia.

Por lo que, resulta esencial que se requiera en la región de procedimientos o autorizaciones especiales que no involucran únicamente a la autoridad y empresas contratantes.

263 Ver: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6900814

264 InternetLab. (2024). Uso de tecnologias espiãs: InternetLab e DataPrivacy Brasil contribuem como *amicus curiae* e participam de audiência pública em caso no STF. InternetLab. https://internetlab.org.br/pt/noticias/uso-de-tecnologias-espias-internetlab-e-dataprivacy-brasil-contribuem-como-amicus-curiae-e-participam-de-audiencia-publica-em-caso-no-stf/

CONCLUSIONES

Los casos enunciados en el Capítulo Tres únicamente representan un pequeño muestreo de un historial de abusos de la vigilancia por parte de los países latinoamericanos, ya sea en forma de recolección masiva e indiscriminada de nuestros datos personales sensibles, *ciberpatrullaje*, el uso de *spywares* contra la sociedad civil, así como muchos otros abusos denunciados.

Dicha práctica genera un **desmantelamiento del espacio cívico**, especialmente el digital, impactando nuestras libertades y autonomía. Por ejemplo, el caso de Colombia es representativo de la manera en la que agencias de seguridad pública e inteligencia contratan servicios privados para el perfilamiento y monitoreo de millones de personas en plataformas digitales, bajo la excusa de prevención e investigación del delito, pero teniendo como fin la recolección de información con fines de control y represión de expresiones críticas del gobierno, así como la difusión de desinformación. Dichos contextos generan un clima de desconfianza digital que restringe la expresión, ya que las personas se autocensuran o limitan su participación digital.

De igual manera, se ha normalizado la **de utilizar medidas intrusivas de vigilancia estatal** (en teoría excepcionales) con retóricas populistas de que "no tenemos nada que esconder" para controlar, censurar y reprimir a la ciudadanía. El caso de Brasil es emblemático en cuanto al uso de sistemas de geolocalización tanto mediante la explotación del SS7 como por medio de sistemas de identificación de placas, visualizando la intensidad con la que se puede afectar la privacidad y libertad de movimiento de millones de personas, trazando perfiles exhaustivos con base en los desplazamientos y rutinas en términos de movimientos de las mismas, incluyendo periodistas, activistas, funcionarias públicas y personas asociadas a investigaciones criminales en contra de familiares del entonces presidente Bolsonaro.

Al perjudicar actividades como el periodismo, la defensa de derechos humanos o la integridad de las instituciones democráticas, **la vigilancia ilegal con frecuencia conlleva una afectación a la sociedad y a sus aspiraciones democráticas,** permitiendo a quien vigila con impunidad ejercer un control e influencia indebida en la sociedad y sus instituciones. El caso de El Salvador es un claro ejemplo de cómo la vigilancia a periodistas compromete a sus fuentes, poniendo en riesgo la revelación de su identidad e incluso su seguridad física. En México, a su vez, existe abundante evidencia del reiterado uso ilegal de herramientas de vigilancia de comunicaciones en contra de personas periodistas, defensoras de derechos humanos, activistas y opositoras políticas.

Adicionalmente, es crucial apreciar que la vigilancia ilegal suele encontrarse aparejada de otras formas de intimidación, desde ataques reputacionales, extorsión, allanamientos, infiltración u operaciones psicológicas hasta potenciar o facilitar agresiones físicas, incluyendo el homicidio.

RECOMENDACIONES A LOS ESTADOS

Con el objetivo de evitar la incertidumbre jurídica y la discrecionalidad en el despliegue de medidas de vigilancia, es necesario que los marcos legales establezcan con mayor exactitud aspectos fundamentales, como la identificación de las autoridades facultadas. Además, deben delimitarse con mayor precisión los parámetros y límites materiales que deben informar las solicitudes de autorización de medidas de vigilancia y las resoluciones judiciales que resuelven dichas solicitudes, a fin de garantizar una mayor previsibilidad sobre los alcances de estas medidas.

Las normas que regulan la vigilancia en los marcos jurídicos regionales fueron diseñadas pensando en tecnologías de intervención telefónica y otras formas de vigilancia focalizada que requerían la colaboración de particulares, especialmente empresas de telecomunicaciones. Por ello, los métodos tradicionales de vigilancia de comunicaciones ofrecían considerablemente menos información de las personas vigiladas y producían ineludiblemente testigos, como lo eran las empresas de telecomunicaciones.

Sin embargo, la proliferación y uso cotidiano de tecnologías de vigilancia masiva cada vez más sofisticadas e invasivas indican que los marcos jurídicos regionales actuales no han sido capaces de asegurar su utilización racional o incluso la posibilidad de que dichas tecnologías puedan siquiera ser compatibles con los principios de necesidad y proporcionalidad previstos en el Capítulo Uno.

En consecuencia, requerimos de voluntad política estatal para que se cumpla con los principios de legalidad, necesidad y proporcionalidad, en línea con los estándares internacionales de derechos humanos previstos para la vigilancia de las comunicaciones, requiriendo que todos los marcos legales nacionales contemplen:

- **Leyes con definiciones claras, precisas y detalladas** de las autoridades facultadas, el procedimiento y circunstancias en las que pueden llevarse a cabo medidas de vigilancia, así como un registro y control del despliegue de medidas de vigilancia estatal.

En línea con los principios de legalidad, finalidad legítima, necesidad y proporcionalidad mencionados en el Capítulo Uno, se requiere de la claridad suficiente para inhibir los abusos en la adquisición y uso de dichas tecnologías de vigilancia, en donde las mismas se encuentren focalizadas a personas específicas y circunscritas a circunstancias en las que haya indicios o causas probables de la comisión de un delito o de una amenaza a la seguridad nacional.

- **Regulación efectiva de los procesos de adquisición** de equipos y sistemas de vigilancia de comunicaciones, con un registro y control de los mismos.
- Medidas de **transparencia**, pues, aún cuando la vigilancia de comunicaciones se encuentra frecuentemente relacionada a la investigación de delitos y amenazas a la seguridad nacional respecto de las cuales cierta secrecía resulta necesaria para su efectividad, la transparencia es esencial para prevenir y detectar abusos, así como para evaluar, con base en evidencia, si los objetivos de interés público que frecuentemente son aludidos para justificar la vigilancia de comunicaciones son conseguidos o si en el despliegue de este tipo de medidas existen actos de corrupción o inadecuados controles frente a potenciales abusos.

El hecho de que muchas de estas tecnologías son utilizadas de manera autónoma por la autoridad atacante, añadido a sus características anti forenses y antidetección, implica un enorme desafío para evitar su utilización ilegal. Por lo que, el establecer obligaciones de publicación de reportes estadísticos, con información desagregada sobre su uso, es particularmente relevante para prevenir, detectar y reparar abusos cometidos por parte de la vigilancia ilegal de comunicaciones.

- Previsión de **salvaguardas** como lo son el control judicial, supervisión independiente y derecho de notificación.

En este contexto, se celebran acciones como la de Brasil en donde organizaciones de sociedad civil solicitaron durante la audiencia pública sobre la ADPF 1.143 que, en caso de que el STF no declare la total inconstitucionalidad del uso de *spyware* por parte de organismos públicos, se establezcan reglas estrictas para evitar sus abusos. También defendieron la exigencia de autorización judicial previa para cualquier monitoreo; la restricción del uso de *spyware* solo cuando no haya otro medio investigativo disponible; la protección del secreto de las comunicaciones; y, la implementación de mecanismos que garanticen la trazabilidad de la cadena de custodia de los datos interceptados.

En países latinoamericanos, con una legacía de autoritarismo y represión de la disidencia, debemos cambiar las narrativas y la percepción pública a un entendimiento compartido en donde equiparemos nuestra privacidad con nuestra seguridad, pues la vigilancia sin controles por autoridades latinoamericanas plagadas por contextos de impunidad y corrupción únicamente implica un mayor control para inhibir las críticas contra el gobierno y para generar miedo, más que para brindarle mayor seguridad a la población.

AlSur

www.alsur.lat