EL ESTADO DE LA VIGILANCIA

R3D
Red en Defensa
de los Derechos Digitales

Unión
Europea

EL ESTADO DE LA VIGILANCIA

R3D
Red en Defensa
de los Derechos Digitales

Unión
Europea

El ESTADO DE LA VIGILANCIA.

Por: Luis Fernando García Muñoz, Ana Gaitán Uribe, José Flores Sosa, Santiago Narváez Herrasti, Milan Trnka Osorio.

Ciudad de México. México, Enero 2025.

Diseño: Gibrán Aquino.

R3D
Red en Defensa de los Derechos Digitales

Unión Europea

Índice

Introducción

Por más de una década, desde **R3D: Red en Defensa de los Derechos Digitales** hemos advertido sobre los riesgos que el creciente uso de tecnologías digitales para la vigilancia de comunicaciones representa para los derechos humanos. También hemos investigado y documentado permanentemente la evidencia de los abusos e utilizado herramientas legales cientos de veces para combatir la opacidad, efectos e impunidad de la vigilancia ilegal.

Por ejemplo, en 2014 desde R3D impugnamos la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR), como resultado de ese juicio de amparo, la Suprema Corte de Justicia de la Nación (SCJN) clarificó por vía interpretativa, las autoridades facultadas para solicitar a empresas de telecomunicaciones información sobre las personas usuarias de esos servicios y explicitó la necesidad de autorización judicial previa para ello.

R3D también ha presentado miles de solicitudes de acceso a la información y centenares de recursos de revisión en materia de transparencia, que han resultado en el acceso de miles de documentos relevantes y que han producido precedentes importantes para el acceso a la información respecto de este tipo de actividades, incluyendo decisiones de la SCJN como la emitida en el Recurso de Revisión en Materia de Seguridad Nacional 1/2016, en el que la SCJN reconoció la publicidad de información estadística sobre medidas de vigilancia o el Amparo en Revisión 105/202, en donde la Segunda Sala de la SCJN estableció que la información en materia de seguridad nacional debe someterse a la prueba de daño.

A lo largo de estos años, R3D ha documentado múltiples abusos de herramienta tecnológicas para la vigilancia. En 2016, publicamos los informes ***El Estado de la Vigilancia: Fuera de Control*** y ***¿Quién defiende tus datos?***, en los que evidenciamos irregularidades y formulamos propuestas para establecer controles democráticos a la vigilancia. En los años siguientes publicamos los informes ***Observatorio de Reportes de Transparencia***, ***¿Quién no defiende tus datos?*** y ***Transparencia y Vigilancia en México***, en los que evidenciamos la insuficiente transparencia sobre las actividades de vigilancia.

Adicionalmente, desde 2017 hemos revelado decenas de casos de espionaje ilegal con tecnologías como el *spyware Pegasus*, en contra de personas defensoras de derechos humanos,

periodistas, activistas y opositores en México mediante investigaciones como ***Gobierno Espía*** y ***Ejército Espía***, acompañando a múltiples víctimas en su búsqueda de justicia y en combate a la impunidad, que a la fecha prevalece.

A partir de esta experiencia, ofrecemos este nuevo informe ***El Estado de la Vigilancia***, en el que recopilamos y ampliamos la evidencia que demuestra que la vigilancia de comunicaciones en México continúa fuera de control.

En primer lugar (*capítulo uno*), se sintetizan los estándares de derechos humanos aplicables a la vigilancia de comunicaciones. Posteriormente (*capítulo dos*), se realiza un análisis de estado actual del marco jurídico mexicano que regula las actividades de vigilancia. A continuación (*capítulo tres*), se presenta un resumen de la evidencia existente sobre las medidas de vigilancia existentes en México, las tecnologías empleadas y sus abusos.

Por último, en los dos capítulos finales, a partir de los hallazgos documentados, se presenta un diagnóstico de los problemas y desafíos que la vigilancia de comunicaciones representa para los derechos humanos y se desarrollan propuestas para el establecimiento de controles democráticos a las medidas de vigilancia de comunicaciones que permitan prevenir, detectar y remediar la sistemática violación de los derechos humanos a través de tecnologías de vigilancia y abatir su impunidad.

Agradecemos especialmente a las víctimas de la vigilancia de comunicaciones en México, cuyo valor y dignidad han permitido a la sociedad conocer y cuestionar los abusos que, desde los pasillos más oscuros del poder público, han sido dirigidos a periodistas, personas defensoras de derechos humanos y otra cuya labor de interés público han contribuido a sostener las aspiraciones democráticas, de justicia y dignidad que continúan pendientes en el país.

Deseamos que este documento, además de preservar la memoria, inspire a la acción para combatir y desmantelar las estructuras que han abusado de su poder para contruir y mantener pactos de impunidad y corrupción que atentan contra los derechos humanos y la democracia.

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 fundamentales reconocidos nacional e internacionalmente. En el ámbito internacional, el derecho a la privacidad se consagra en la 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) y la Convención Internacional sobre la Protección de los Derechos de todos los Trabajadores Migratorios y de sus Familiares (art. 14).

El Comité de Derechos Humanos de la Organización de las Naciones Unidas (en adelante, "CDH") ha reconocido en su Observación General Número 16 que, conforme al artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, toda persona tiene derecho a ser protegida respecto de injerencias ilegales o arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, así como de ataques ilegales a su honra y reputación.

A nivel interamericano, el derecho a la vida privada y la protección de datos personales están protegidos por el artículo 11 de la Convención Americana de Derechos Humanos (en adelante, "CADH"). Así, la Corte Interamericana de Derechos Humanos (en adelante, "Corte IDH") ha definido a la vida privada como:

> *[...] un concepto amplio que no es susceptible de definiciones exhaustivas y comprende, entre otros ámbitos protegidos, la vida sexual y el derecho a establecer y desarrollar relaciones con otros seres humanos. Es decir, la vida privada incluye la forma en que el individuo se ve a sí mismo y cómo y cuándo decide proyectar a los demás.*[1]

En términos casi idénticos a los del CDH, la Corte IDH ha señalado que el artículo 11 de la CADH prohíbe toda injerencia arbitraria o abusiva en la vida privada de las personas, enunciando diversos ámbitos de protección del derecho, como la vida privada de sus familias, sus domici-

1. Corte IDH. Caso *Atala Riffo y Niñas Vs. Chile*. Fondo, Reparaciones y Costas. Sentencia del 24 de febrero de 2012. Serie C No. 239, Párrafo 164.

lios, correspondencias o comunicaciones.[2] En tal sentido, se ha considerado que el ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública.[3]

Por su parte, el Tribunal Europeo de Derechos Humanos (en adelante, "TEDH") también ha interpretado que la noción de privacidad no tiene una definición exhaustiva. En el caso *López Ribalda y otros contra España* determinó que la vida privada engloba la integridad física y psicológica de una persona, pudiendo incluir múltiples aspectos de su identidad social y física. En ese orden de ideas, concluyó que sería muy restrictivo limitar dicha noción a un círculo íntimo, pues el individuo necesita vivir su vida personal como guste e incluir y excluir a las demás de dicho círculo.

Ahora bien, conforme a los Principios Actualizados del Comité Jurídico Interamericano sobre la Privacidad y la Protección de Datos Personales, con Anotaciones, la definición de ***datos personales*** abarca *"la información que identifica o puede usarse de manera razonable para identificar a una persona física de forma directa o indirecta", lo que incluye los distintos "factores referidos específicamente a su identidad física, fisiológica, genética, mental, económica, cultural o social [...] expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica, electrónica, visual o de cualquier otro tipo".*[4]

En esta línea, la Corte IDH establece que:

> *[...] los estándares internacionales en materia de protección de datos personales exigen que su recopilación, almacenamiento, tratamiento y divulgación sea factible solamente ante el consentimiento libre e informado del titular de los datos o, en su defecto, derivado de un marco normativo que faculte expresamente a los organismos públicos para desarrollar tales acciones.*[5]

Al respecto, es importante recalcar que la protección que toda persona tiene 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.**[6]

---

2. Corte IDH. Caso de las *Masacres de Ituango Vs. Colombia*. Sentencia de 1 de julio de 2006. Serie C No. 148, párr. 193, y Caso Manuela y otros Vs. El Salvador. Excepciones preliminares, Fondo, Reparaciones y Costas. Sentencia de 2 de noviembre de 2021. Serie C No. 441, párr. 204.

3. Corte IDH. Caso de las *Masacres de Ituango Vs. Colombia*, supra, párrs. 193 y 194, y Caso *Tzompaxtle Tecpile y otros Vs. México*. Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia de 7 de noviembre de 2022. Serie C No. 470, párr. 189.

4. Principios Actualizados del Comité Jurídico Interamericano sobre la Privacidad y la Protección de Datos Personales, con Anotaciones, pág. 23. Véase también, Opinión Consultiva OC-24/17, párr. 123.

5. 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.

6. 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]).

Como observó el entonces Alto Comisionado de las Naciones Unidas para los Derechos Humanos en su innovador informe de 2014 sobre "*El derecho a la privacidad en la era digital*" —adoptado por consenso por los miembros de la Asamblea General de la ONU el 18 de diciembre de 2013—, tanto el contenido de las comunicaciones como los metadatos —es decir, los datos sobre las comunicaciones como quiénes, cuándo, cómo, por cuánto tiempo, en dónde— están protegidos por el derecho a la privacidad, ya que los metadatos también pueden revelar información sobre el comportamiento de las personas y permitir extraer conclusiones sobre su vida privada.[7]

La Corte IDH también se ha pronunciado en cuanto a la protección de la vida privada en el marco de los metadatos, recalcando que sus criterios *"tienen plena aplicación en torno a actividades de inteligencia que supongan una vigilancia de [dichos metadatos]"*. En tal sentido, ha señalado que (énfasis añadido):

> *[...] si bien las conversaciones telefónicas no se encuentran expresamente previstas en el artículo 11 de la Convención, se trata de una forma de comunicación que, al igual que la correspondencia, se encuentra incluida dentro del ámbito de protección del derecho a la vida privada.*[8] *Asimismo, ha indicado que* ***el alcance del citado artículo 11 se aplica a las conversaciones telefónicas independientemente de su contenido e incluso, puede comprender tanto las operaciones técnicas dirigidas a registrar ese contenido, mediante su grabación y escucha, como cualquier otro elemento del proceso comunicativo mismo, por ejemplo, el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas, aspectos que pueden ser constatados sin necesidad de registrar el contenido de la llamada mediante la grabación de las conversaciones.*** *En definitiva, a juicio de esta Corte, la protección a la vida privada se concreta en el derecho a que sujetos distintos de los interlocutores no conozcan ilícitamente el contenido de las conversaciones telefónicas o de otros aspectos, como los ya mencionados, propios del proceso de comunicación.*[9]

Asimismo, el Relator Especial sobre la Promoción y Protección del Derecho a la Libertad de Expresión de la Organización de las Naciones Unidas (en adelante, "ONU") ha hecho referencia al carácter sumamente revelador e invasivo del análisis de dichos datos en el siguiente sentido (énfasis añadido):

> *El carácter dinámico de la tecnología no solo ha cambiado la forma en que puede llevarse a cabo la vigilancia, sino también "qué" puede vigilarse. Al facilitar la creación de oportunidades de comunicación e intercambio de información, Internet también ha posibilitado la elaboración de un gran volumen de datos de transacciones de personas y acerca de estas. Esta información, conocida como datos de las comunicaciones o metadatos,* ***incluye información personal sobre particulares, su ubicación y actividades en línea, así como registros e información conexa sobre los correos electrónicos y los mensajes que envían o reciben.*** *Los datos de las comunicaciones pueden almacenarse, son accesibles y permiten*

7. A/HRC/27/37, 30 de junio de 2014, pár. 19.

8. Corte IDH. Caso Tristán Donoso Vs. Panamá. Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia de 27 de enero de 2009. Serie C No. 193, párr. 55; y, Caso Escher y otros vs. Brasil. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 6 de julio de 2009. Serie C No. 200, párr. 114.

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

> *la realización de búsquedas y su revelación a las autoridades públicas y su utilización por éstas están en gran medida no reguladas.* ***El análisis de estos datos puede ser sumamente revelador e invasivo, en particular cuando los datos se combinan y acumulan.*** *En tal sentido, los Estados se basan cada vez más en datos de las comunicaciones para prestar apoyo a las investigaciones de las fuerzas del orden o de seguridad nacional. Los Estados también están disponiendo la obligatoriedad de conservar y retener los datos de las comunicaciones para poder llevar a cabo una vigilancia histórica.*

Al respecto, el Grupo de Trabajo Sobre Protección de Datos (ahora Comité Europeo de Protección de Datos [en adelante, "CEPD"]), del Parlamento Europeo ha reconocido la gran cantidad de información íntima que recopilan nuestros dispositivos móviles. En efecto, el Comité Europeo señala que: *"[l]os dispositivos móviles inteligentes están muy estrechamente vinculados a las personas porque la mayoría de ellas tienden a mantener su dispositivo móvil muy cerca de ellas, en el bolsillo, en el bolso o sobre la mesilla de noche".*

En la misma línea, el Tribunal de Justicia de la Unión Europea (en adelante "TJUE") ha sostenido lo siguiente con respecto a los metadatos:

> *[...] pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los medios sociales que frecuentan.*[10]

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 amenazas a la seguridad nacional. No obstante, la jurisprudencia interamericana ha conocido de distintos casos en los que los servicios de inteligencia estatales, excediéndose en las facultades que legítimamente pueden ejercer en un sistema democrático, han incurrido en distintas violaciones a los derechos humanos.[11]

---

10. TJUE. *Digital Rights Irlanda vs. Ministro de Comunicaciones, Casos Conjuntos*, C-293/12 y C-594/12, 8 de abril de 2014, párr. 26.

11. 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.

En este sentido, la Corte IDH ha establecido que las actividades de inteligencia comprenden:

> *[...] distintas tareas, emprendidas mediante diferentes mecanismos y estrategias, dirigidas al rastreo, obtención, recopilación, clasificación, sistematización, procesamiento, registro, utilización, evaluación, análisis, interpretación, producción y difusión de información de distinto tipo, incluidos datos personales.*[12]

Recientemente, en el *Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia* (en adelante, "caso CAJAR")[13], la Corte IDH analizó los estándares aplicables al respeto de los derechos humanos en el desarrollo de actividades de inteligencia realizadas por el Estado y determinó lo siguiente:

> *El recuento de los criterios aplicables a las actividades de inteligencia hace necesario tener presente el alcance de los derechos humanos y las limitaciones que legítimamente pueden imponerse a estos. Lo anterior se explica a partir de la íntima relación que existe entre las acciones propias que en el marco de la inteligencia estatal se desarrollan y los derechos humanos, entendida en doble vía: a) por un lado, las actividades de inteligencia necesariamente deben conducirse al objetivo último de proteger a las personas que habitan en el territorio del Estado, lo que incluye la salvaguarda de sus derechos y libertades, y b) por el otro, el ejercicio mismo de las actividades de inteligencia, dados los medios empleados y su incidencia en la obtención y utilización de información, incluidos datos personales, supone una injerencia en la esfera de derechos de la persona, en particular del derecho a la vida privada, todo lo cual torna imprescindible delimitar las exigencias, requisitos y controles que se imponen para hacer compatibles aquellas actividades con las condiciones y fines de un Estado de Derecho y, con ello, con el contenido de la Convención Americana.*

Organismos internacionales como la ONU[14] y la Organización de los Estados Americanos (en

---

12. 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, par. 525.

13. 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.

14. Consejo de Derechos Humanos, 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, Recopilación de buenas prácticas relacionadas con los marcos y las medidas de carácter jurídico e institucional que permitan garantizar el respeto de los derechos humanos por los servicios de inteligencia en la lucha contra el terrorismo, particularmente en lo que respecta a su supervisión, U.N. Doc. A/HRC/14/46, 17 de mayo de 2010 (en adelante "Buenas prácticas para garantizar los derechos humanos por los servicios de inteligencia, A/HRC/14/46"). Consejo de Derechos Humanos, Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue, U.N. Doc. A/HRC/23/40, 17 de abril de 2013 (en adelante "Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, A/HRC/23/40") Consejo de Derechos Humanos, El derecho a la privacidad en la era digital, Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, U.N. Doc. A/HRC/27/37, 30 de junio de 2014 (en adelante "El derecho a la privacidad en la era digital, Informe de OACNUDH, A/HRC/27/37"), y Asamblea General de las Naciones Unidas, El derecho a la privacidad en la era digital, U.N. Doc. A/RES/75/176, 28 de diciembre de 2020 (en adelante "Resolución de la Asamblea General, A/RES/75/176").

adelante, "OEA")[15], así como organizaciones de la sociedad civil[16], han identificado un conjunto de estándares, principios y criterios a los que deben estar sometidas las actividades de inteligencia para afirmar su validez, legitimidad en un sistema democrático y compatibilidad con los derechos humanos y con la Convención Americana.

Conforme a los "Principios Necesarios y Proporcionados sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones", la ***vigilancia de las comunicaciones*** en el entorno moderno comprende monitorear, interceptar, recoger, analizar, usar, preservar, guardar, interferir u obtener información que incluya o refleje las comunicaciones pasadas, presentes o futuras de una persona, se derive o surja de ellas.[17]

En el caso de *Myrna Mack Chang Vs. Guatemala*, 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"*.[18] El criterio fue reiterado en el caso *Hermanos Landaeta Mejías y otros Vs. Venezuela.*[19]

De igual manera, indicó en el caso CAJAR que la trascendencia de identificar las exigencias y controles a los que deben estar sometidas las actividades de inteligencia para afirmar su validez y legitimidad en un sistema democrático se revela (énfasis añadido):

> *[...] no solo por la inminente fricción que surge entre las actividades de inteligencia y los derechos de la persona, sino también porque de ordinario este tipo de operaciones, para asegurar la eficaz realización de sus cometidos,* ***se ejecutan de forma reservada o en secreto, sin el conocimiento de la población en general y sin el consentimiento de quienes podrían resultar directamente afectados, aumentando el riesgo de un ejercicio abusivo o arbitrario del poder público.***[20]

Así, para que las restricciones a los derechos a la privacidad y a la protección de datos personales cumplan con los estándares nacionales e internacionales en la materia —y prohíban medidas de vigilancia encubierta—, deben cumplir con los requisitos de legalidad, finalidad legí-

---

15. 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.

16. Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. Disponibles en: https://necessaryandproportionate.org/es/13-principles/

17. *Ibid.*

18. 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.

19. Corte IDH. Caso *Hermanos Landaeta Mejías y otros Vs. Venezuela*. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 27 de agosto de 2014. Serie C No. 281, párr. 126.

20. 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, par. 527.

tima, 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

El CDH ha determinado que, al aprobar leyes que prevean restricciones permitidas en virtud de finalidades legítimas, los Estados deben (énfasis añadido):

> *[...] guiarse siempre por* ***el principio de que las restricciones no deben comprometer la esencia del derecho*** *[...] no se debe invertir la relación entre derecho y restricción, entre norma y excepción. Las leyes que autoricen la aplicación de restricciones* ***deben utilizar criterios precisos y no conferir una discrecionalidad sin trabas a los encargados de su aplicación.***[22]

De igual manera, ha señalado que cualquier *"injerencia autorizada por los Estados"* en la vida privada de las personas *"solo puede tener lugar en virtud de la ley, que a su vez debe conformarse a las disposiciones, propósitos y objetivos del Pacto"*, y debe ser *"razonable en las circunstancias particulares del caso"*.[23]

En esta línea, el Relator Especial de las Naciones Unidas para la Protección y Promoción del Derecho a la Libertad de Expresión y la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (en adelante, "CIDH") apuntaron en su Declaración Conjunta sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión lo siguiente (énfasis añadido):

> *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****.*

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. CDH, Comentario General 27, pár. 13.

23. Recopilación de las observaciones generales y recomendaciones generales adoptadas por órganos creados en virtud de tratados de derechos humanos, Observación general No. 16 del Comité de Derechos Humanos: Artículo 17 - Derecho a la intimidad, U.N. Doc. HRI/GEN/1/Rev.7, 12 de mayo de 2004, párrs. 3 y 4 (en adelante "Observación general No. 16 del Comité de Derechos Humanos")

La misma Relatoría ha establecido que, en el contexto de medidas de vigilancia encubierta, 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]

El TEDH se ha pronunciado en términos exactos en el contexto de medidas de vigilancia encubierta, como la geolocalización en tiempo real de equipos de comunicación móvil o el acceso a metadatos de comunicaciones.[25] Además, ha señalado que, en vista del riesgo de abuso que cualquier sistema de vigilancia secreta implica, las medidas deben basarse en una ley que sea particularmente precisa, en vista de que la tecnología disponible para realizar esas actividades continuamente se vuelve más sofisticada.[26]

En igual sentido, la Relatoría Especial para la Libertad de Expresión de la CIDH ha apuntado que (énfasis añadido):

> ***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.*
>
> *[...] Las leyes que habiliten la intercepción de las comunicaciones deben establecer con claridad y precisión las causas que el Estado puede invocar para solicitar esa intercepción, que sólo puede ser autorizada por un juez. Asimismo, se deben establecer por ley garantías vinculadas a la naturaleza, alcance y duración de las medidas de vigilancia; los hechos que podrían justificar esas medidas y las autoridades competentes para autorizarlas, llevarlas a cabo y supervisarlas. La ley debe ser clara en cuanto a posibles remedios para los abusos cometidos en el ejercicio de esas facultades.*[27]

En la misma línea, la Corte IDH ha señalado que la primera exigencia en el ejercicio de actividades de inteligencia se refiere al ***principio de reserva de ley***, mismo que conforma *"un elemento esencial para que los derechos [...] est[én] jurídicamente protegidos y exist[an] plenamente en la realidad"*, a la vez que *"garanti[za] eficazmente [...] un control adecuado del ejercicio de las competencias de los órganos"* estatales.[28]

---

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. TEDH, Caso de *Uzun vs. Alemania*, Aplicación No. 35623/05, sentencia de 2 de septiembre de 2010, párr. 61; Caso de *Valenzuela Contreras vs. España*, Aplicación No. 58/1997/842/1048, sentencia de 30 de julio de 1998, párr. 46.

26. TEDH, Caso de *Uzun vs. Alemania, ibid; Weber y Sarabia vs. Alemania*, Aplicación No. 54934/00, decisión de 29 de junio de 2006, párr. 93.

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

28. 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, par. 529.

Por lo que, en cuanto al marco legal específico para actividades de inteligencia, la Corte IDH determina que se deben definir con precisión las mismas, así como los fines que por su medio deben perseguirse y las facultades de los órganos y autoridades competentes.[29] En tal sentido, las leyes deben prever:

> *[...] con la mayor precisión posible, las distintas amenazas que determinan la necesidad de emprender las actividades de inteligencia por parte de los agentes estatales con competencia en la materia, cuyas facultades también deben estar clara y exhaustivamente establecidas, a fin de limitar eficazmente su actuar, impedir la arbitrariedad en su proceder y posibilitar su control y la eventual deducción de responsabilidades.*[30]

En efecto, en cuanto a los controles y limitaciones a los que deben ser sometidas las actividades de inteligencia, la Corte IDH determinó en el caso CAJAR lo siguiente (énfasis añadido):

> *[...] es menester que la legislación interna* ***delimite, con la mayor precisión posible, los siguientes aspectos: a) los tipos de medidas y acciones de obtención y recopilación de información autorizadas en materia de inteligencia; b) los objetivos perseguidos con tales medidas; c) las clases de personas y actividades respecto de las cuales se permite obtener y recopilar información, en función, claro está, de la identificación de amenazas para la realización de los fines legítimos antes identificados; d) el grado de sospecha que puede justificar la obtención y recopilación de información; e) los plazos dentro de los cuales se permite el empleo de las citadas medidas y estrategias, y f) los métodos útiles para actualizar, supervisar y examinar las medidas y acciones empleadas para obtener y recopilar información.***[31]
>
> *En el caso de que la legislación acepte el intercambio de información entre organismos de inteligencia del mismo o de otro Estado, la regulación debe precisar las condiciones para ello, los finales que habilitan el intercambio, las entidades autorizadas y las salvaguardas necesarias para la seguridad de la información (especialmente los datos personales).*[32]
>
> *La necesidad de asegurar mecanismos efectivos de* ***control [...] exige la formalización, por medio de procesos numerados, de las distintas actividades de inteligencia emprendidas, con el debido registro de todas sus etapas, incluido el historial de registros de acceso a sistemas electrónicos.*** *Asimismo, en el caso del procesamiento de datos personales obtenidos por los organismos de inteligencia, las salvaguardas en esta materia [...] hacen necesario que, en la medida de lo posible, se mantenga* ***un registro que (i) identifique a los responsables de dicho procesamiento; (ii) los propósitos para el procesa-***

---

29. Buenas prácticas para garantizar los derechos humanos por los servicios de inteligencia, A/HRC/14/46, Prácticas 2 y 20, y El derecho a la privacidad en la era digital, Informe de OACNUDH, A/HRC/27/37, párr. 23.

30. Buenas prácticas para garantizar los derechos humanos por los servicios de inteligencia, A/HRC/14/46, Prácticas 3 y 4, y El derecho a la privacidad en la era digital, Informe de OACNUDH, A/HRC/27/37, párr. 23.

31. Buenas prácticas para garantizar los derechos humanos por los servicios de inteligencia, A/HRC/14/46, Prácticas 20 y 21, y El derecho a la privacidad en la era digital, Informe de OACNUDH, A/HRC/27/37, párr. 28; y, TEDH, Caso Huvig Vs. Francia, No. 11105/84, Sentencia de 24 de abril de 1990, párr. 34.

32. Buenas prácticas para garantizar los derechos humanos por los servicios de inteligencia, A/HRC/14/46, Prácticas 31, 32 y 33.

> ***miento de la información recopilada, indicando el origen y categoría de los datos; (iii) la base jurídica de las operaciones realizadas; (iv) los plazos de conservación, y (v) las técnicas utilizadas para su tratamiento. Las operaciones con datos personales también deberán llevar registros cronológicos de acceso, alteración, consulta, eliminación o divulgación de tales datos, así como de las personas que accedieron a ellos.***[33]

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 en los términos siguientes:

> *Dicha ley debe regular, con la mayor precisión posible, lo siguiente: 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 [...].*[34]

Finalmente, los ***principios de legalidad y seguridad jurídica*** están previstos en el ordenamiento mexicano en los artículos 14 y 16 de la Constitución y obligan a las autoridades a fundar y motivar las intromisiones en la esfera jurídica de las personas en virtud de un mandamiento escrito emitido por la autoridad competente. Dichos principios tutelan que las personas gobernadas jamás se encuentren en una situación de incertidumbre jurídica que se traduzca en un estado de indefensión.

La Suprema Corte de Justicia de la Nación (en adelante, "SCJN") ha determinado que el legislador respeta los derechos fundamentales de legalidad y seguridad jurídica cuando las normas que facultan a las autoridades para actuar en determinado sentido cumplen con los siguientes requisitos:[35]

a) La persona gobernada conoce cuál será la consecuencia jurídica de los actos que realice; y,

---

33. Buenas prácticas para garantizar los derechos humanos por los servicios de inteligencia, A/HRC/14/46, Prácticas 6, 22, 24 y 31. Véase, artículos 24 y 25 de la Directiva relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos, Parlamento Europeo y Consejo de la Unión Europea, (UE) 2016/680, 27 de abril de 2016.Disponible en: https://www.boe.es/doue/2016/119/L00089-00131.pdf

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. 577.

35. SCJN. Amparo directo en revisión 3441/2013. Comaxim, S.A. de C.V. Resuelto el 8 de enero de 2014. Ponente: José Fernando Franco González Salas. Cinco votos de los Ministros Sergio A. Valls Hernández, Alberto Pérez Dayán, José Fernando Franco González Salas, Margarita Beatriz Luna Ramos y Luis María Aguilar Morales.

b) El actuar de la respectiva autoridad se encuentra limitado y acotado para evitar afectaciones arbitrarias o caprichosas en la esfera jurídica de las personas.[36]

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

A. Finalidad constitucionalmente válida

El Relator Especial de la ONU para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión ha reconocido que la protección de la seguridad nacional puede justificar el uso excepcional de la vigilancia en las comunicaciones privadas.[37] No obstante, aun 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 de identificar los fines que persiguen para después poder determinar si son constitucionalmente válidos.[38] Así, las leyes solo 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 CDH (énfasis añadido):

> *Los gobiernos suelen alegar que los programas de vigilancia de las comunicaciones digitales obedecen a motivos de seguridad nacional, en particular los riesgos planteados por el terrorismo. En varias de las contribuciones se indicó que, puesto que las tecnologías de comunicación digital pueden ser, y han sido, utilizadas por particulares con fines delictivos (como el reclutamiento para la comisión de atentados terroristas y el financiamiento de los mismos), la vigilancia legal y específica de las comunicaciones digitales puede constituir una medida necesaria y eficaz para las entidades de inteligencia y/o de aplicación de la ley cuando se lleva a cabo en cumplimiento de la legislación internacional y nacional.* ***La vigilancia por motivos de seguridad nacional o para prevenir atentados terroristas u otros delitos puede ser un "objetivo legítimo" a los efectos de***

36. SCJN. Tesis: 2ª./J, 106/2017 (10ª.) Registro: 2014864. "DERECHOS FUNDAMENTALES DE LEGALIDAD Y SEGURIDAD JURÍDICA. SU CONTRAVENCIÓN NO PUEDE DERIVAR DE LA DISTINTA REGULACIÓN DE DOS SUPUESTOS JURÍDICOS ESENCIALMENTE DIFERENTES".

37. ONU. Relator Especial de las Naciones Unidas para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión, Informe sobre vigilancia de comunicaciones y sus implicaciones en el ejercicio de los derechos a la privacidad y libertad de expresión, A/HRC/23/40.

38. 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

> ***realizar una evaluación desde el punto de vista del artículo 17 del Pacto. Sin embargo, el grado de injerencia debe contraponerse a la necesidad de la medida para lograr ese objetivo y el beneficio real que se obtiene a tal efecto.***[39]

En la misma línea, en la referida *Declaración Conjunta sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión*, los Relatores de la ONU afirmaron lo siguiente (énfasis añadido):

> *Dada la importancia del ejercicio de estos derechos para el sistema democrático, la ley debe autorizar el acceso a las comunicaciones y a datos personales sólo en las circunstancias más excepcionales definidas en la legislación.* ***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.*** *La entrega de esta información debe ser monitoreada por un organismo de control independiente y contar con garantías suficientes de debido proceso y supervisión judicial, dentro de las limitaciones permisibles en una sociedad democrática.*

El propio contenido de la Convención Americana denota cuáles habrán de considerarse fines legítimos que autorizan la restricción de derechos (artículos 13, 15, 16 y 22 de la Convención, en armonía con el texto del Pacto Internacional de Derechos Civiles y Políticos, artículos 12, 14, 19, 21 y 22). **De esa cuenta, de acuerdo con la Corte IDH, serán fines legítimos en este ámbito los siguientes: a) la protección de la seguridad nacional; b) el mantenimiento del orden público; c) la salvaguarda de la salud pública, y, d) la protección de los derechos humanos.**[40]

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.[41] 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.[42] Así:

> ***Por consiguiente, las "amenazas" que, según el marco legal interno, habilitarían la ejecución de las actividades de inteligencia deben referirse, forzosamente, a factores o situaciones que de manera racional y concreta podrían poner en riesgo la realización de aquellos fines legítimos, fuera***

39. A/HRC/27/37, pár. 24.

40. 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, par. 531.

41. *Ibidem*, pár. 533.

42. *Ibidem*, pár. 532.

de los cuales no es lícito que las autoridades estatales emprendan acciones o estrategias en este ámbito.[43] Ello determina la necesidad, como ha sido indicado, de que la ley precise aquellos fines, a la vez que identifique las eventuales amenazas a estos, cuya prevención o neutralización es el propósito de las actividades de inteligencia, evitando con ello el ejercicio desmedido de las facultades estatales, máxime en un ámbito en el que, como también ha sido adelantado, el riesgo de arbitrariedad se incrementa dada la naturaleza del quehacer estatal y el carácter reservado que regularmente se impone.[44]

B. Idoneidad de la medida

En segundo lugar, la grada de ***idoneidad***[45] determina si la medida impugnada es adecuada para alcanzar los fines perseguidos por el legislador o la autoridad. 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 SCJN 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"*.[46]

C. Necesidad de la medida

La vigilancia de las comunicaciones solo 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.

---

43. Véase, TEDH, inter alia, *Caso Klass y otros Vs. Alemania*, No. 5029/71, Sentencia de 6 de septiembre de 1978, párr. 51; Caso *Kennedy Vs. Reino Unido*, No. 26839/05, Sentencia de 18 de mayo de 2010, párrs. 31 y 32, y Caso *Roman Zakharov Vs. Rusia* [GS], No. 47143/06, Sentencia de 4 de diciembre de 2015, párr. 260.

44. 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, par. 534 Buenas prácticas para garantizar los derechos humanos por los servicios de inteligencia, A/HRC/14/46, Prácticas 1, 2 y 3, y El derecho a la privacidad en la era digital, Informe de OACNUDH, A/HRC/27/37, párr. 29. Véase, Consejo de Derechos Humanos, Informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Martin Scheinin, U.N. Doc. A/HRC/13/37, 28 de diciembre de 2009, párr. 60, y Consejo de Derechos Humanos, El derecho a la privacidad en la era digital, Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, U.N. Doc. A/HRC/39/29, 3 de agosto de 2018, párr. 35.

45. 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.

46. 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

Para lo anterior, conforme a la Suprema Corte de Justicia de la Nación, es necesario corroborar dos elementos:

I. Si existen otros medios con un grado de idoneidad igual o superior para lograr los fines perseguidos; y,

II. Si estas medidas intervienen con menor intensidad en el derecho fundamental afectado.[47]

En el amparo 237/2014, la Primera Sala de la SCJN estableció que en el escrutinio de medidas alternativas pueden ponderarse las medidas que el legislador consideró adecuadas para situaciones similares. Por lo que, en el primer paso de la grada de necesidad, se analiza si existen medidas que sean iguales, más eficaces, rápidas y/o con mayor probabilidad de éxito, así como medidas que tengan menor afectación material del objeto perseguido.

El segundo paso de estudio de la grada de necesidad consiste en analizar si la medida propuesta es menos lesiva. En este sentido, lo principalmente problemático al emplear tecnologías de vigilancia de comunicaciones se centra en su usual amplia naturaleza. Así, distintos relatores de Naciones Unidas y tribunales regionales de derechos humanos han reiterado en sus declaraciones que las tecnologías de vigilancia masiva son incompatibles con el derecho a la privacidad.[48]

Por ejemplo, el Tribunal de Justicia de la Unión Europea (en adelante, "TJUE") ha considerado que las medidas que obligan a la recolección y conservación masiva e indiscriminada de datos personales son incompatibles con el derecho a la privacidad y a la protección de datos en el sentido siguiente (énfasis añadido):

> *[L]a Directiva 2006/24 abarca de manera generalizada a todas las personas, medios de comunicación electrónica y datos relativos al tráfico sin que se establezca ninguna diferenciación, limitación o excepción en función del objetivo de lucha contra los delitos graves.*
>
> *En efecto, por una parte, la Directiva 2006/24* ***afecta con carácter global a todas las personas que utilizan servicios de comunicaciones electrónicas, sin que las personas cuyos datos se conservan se encuentren, ni siquiera indirectamente, en una situación que pueda dar lugar a acciones penales.***

---

47. SCJN. Primera Sala de la Suprema Corte de Justicia de la Nación. Amparo en revisión 237/ 2014. Ponente: Arturo Zaldívar Lelo de Larrea. Aprobado por mayoría de votos. De esta sentencia se emitió la Tesis Aislada CCLXX/2016 (10a.) "TERCERA ETAPA DEL TEST DE PROPORCIONALIDAD. EXAMEN DE LA NECESIDAD DE LA MEDIDA LEGISLATIVA." Registro: 2013154

48. *Véanse*, A/69/397 (23 de septiembre de 2014); Relator Especial de la ONU sobre la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión y Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, Declaración Conjunta sobre los Programas de Vigilancia y su Impacto en la Libertad de Expresión (21 de junio de 2013); Tribunal de Justicia de la Unión Europea en el asunto C-362/14 Schrems c. Comisario de Protección de Datos ECLI: EU:C:20-15:650; y el Tribunal Europeo de Derechos Humanos, más recientemente en Big Brother Watch and ors v United Kingdom [2021] ECHR 439 (GC).

Por lo tanto, se aplica incluso a personas respecto de las que no existen indicios que sugieran que su comportamiento puede guardar relación, incluso indirecta o remota, con delitos graves. Además, no establece ninguna excepción, por lo que se aplica también a personas cuyas comunicaciones están sujetas al secreto profesional con arreglo a las normas de la legislación nacional.

Por otra parte, aun cuando la Directiva pretende contribuir a la lucha contra la delincuencia grave, ***no exige ninguna relación entre los datos cuya conservación se establece y una amenaza para la seguridad pública y, en particular, la conservación no se limita a datos referentes a un período temporal o zona geográfica determinados o a un círculo de personas concretas que puedan estar implicadas de una manera u otra en un delito grave, ni a personas que por otros motivos podrían contribuir, mediante la conservación de sus datos, a la prevención, detección o enjuiciamiento de delitos graves.***

En segundo lugar, a esta falta general de límites se añade que la Directiva 2006/24 no fija ningún criterio objetivo que permita delimitar el acceso de las autoridades nacionales competentes a los datos y su utilización posterior con fines de prevención, detección o enjuiciamiento de delitos que, debido a la magnitud y la gravedad de la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta, puedan considerarse suficientemente graves para justificar tal injerencia. Por el contrario, la Directiva 2006/24 se limita a remitir de manera general, en su artículo 1, apartado 1, a los delitos graves tal como se definen en la legislación nacional de cada Estado miembro.

(...) En tercer lugar, en lo que atañe al período de conservación de los datos, la Directiva 2006/24 prescribe, en su artículo 6, la conservación de éstos durante un período mínimo de seis meses ***sin que se establezca ninguna distinción entre las categorías de datos*** *previstas en el artículo 5 de la Directiva en función de su posible utilidad para el objetivo perseguido o de las personas afectadas.*

(...) De lo anterior resulta que la Directiva 2006/24 no establece reglas claras y precisas que regulen el alcance de la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta. Por lo tanto, ***debe considerarse que esta Directiva constituye una injerencia en los derechos fundamentales de gran magnitud y especial gravedad en el ordenamiento jurídico de la Unión,*** *sin que esta injerencia esté regulada de manera precisa por disposiciones que permitan garantizar que se limita efectivamente a lo estrictamente necesario.*[49]

Igualmente, en el *Caso Watson y otros* resolvió que:

[S]i bien es cierto que la eficacia de la lucha contra la delincuencia grave, especialmente contra la delincuencia organizada y el terrorismo, puede depender en gran medida del uso de técnicas modernas de investigación, este objetivo de interés general, por muy fundamental que sea, no puede por sí solo justificar que una normativa nacional que establezca la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización deba ser considerada necesaria a los efectos de dicha lucha (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 51).

49. TJUE. Digital Rights Ireland vs. Minister of Communications, Marine and Natural Resources y otros. Casos Conjuntos, C-293/12 y C-594/12, 8 de abril de 2014.

A este respecto, debe señalarse, por una parte, que una normativa de este tipo tiene como consecuencia, habida cuenta de sus características, descritas en el apartado 97 de la presente sentencia, que la conservación de los datos de tráfico y de localización se convierta en la regla, mientras que el sistema creado por la Directiva 2002/58 exige que esa conservación de datos sea excepcional.

Por otra parte, una normativa nacional, como la controvertida en el asunto principal, que cubre de manera generalizada a todos los abonados y usuarios registrados y que tiene por objeto todos los medios de comunicación electrónica así como todos los datos de tráfico, no establece ninguna diferenciación, limitación o excepción en función del objetivo que se pretende lograr. Esta normativa afecta globalmente a todas las personas que hacen uso de servicios de comunicaciones electrónicas, aunque no se encuentren, ni siquiera indirectamente, en una situación que justifique una acción penal. Por tanto, esa normativa se aplica incluso a las personas de las que no existe ningún indicio para pensar que su comportamiento pueda tener una relación, incluso indirecta o remota, con la comisión de delitos graves. Además, no establece ninguna excepción, por lo que se aplica también a personas cuyas comunicaciones están sujetas a secreto profesional conforme al Derecho nacional (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartados 57 y 58).

Una normativa de este tipo no exige ninguna relación entre los datos cuya conservación se establece y una amenaza para la seguridad pública. En particular, no está limitada a una conservación de datos referentes a un período temporal, una zona geográfica o un círculo de personas que puedan estar implicadas de una manera u otra en un delito grave, ni a personas que por otros motivos podrían contribuir, mediante la conservación de sus datos, a la lucha contra la delincuencia (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 59).

Una normativa nacional como la controvertida en el asunto principal excede, por tanto, de los límites de lo estrictamente necesario y no puede considerarse justificada en una sociedad democrática, como exige el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta.[50]

Además, el anterior Relator Especial sobre la libertad de opinión y de expresión, David Kaye, también ha enfatizado preocupaciones en cuanto al empleo de sofisticadas herramientas de vigilancia conocidas como spyware, mismas que, a pesar de que suelen dirigirse específicamente contra una persona, usualmente recopilan información sobre ella y sus contactos de manera desproporcionada y excesiva.[51] En esta línea, la Relatora Especial sobre la Lucha contra el Terrorismo ha indicado lo siguiente (traducido por cuenta propia del inglés al español):

[...] las capacidades inherentes del spyware, que permiten un control absoluto sobre la totalidad de la vida digital de un sujeto, pueden hacer imposible que los usos de la tecnología cumplan con los requisitos de que cualquier vigilancia debe limitarse a lo que sea necesario y proporcionado para la

50. TJUE. Watson y otros. Vs Secretary of State for the Home Department y otros. Casos Conjuntos, C-203/15 y C-698/15, 21 de diciembre de 2016.

51. Profesor D. Kaye, 'Here's what world leaders must do about spyware,' 13 de octubre de 2022, Committee to Protect Journalists, disponible en: https://cpj.org/2022/10/david-kaye-what-world-leaders-must-do-about-spyware/

persecución de una finalidad legítima. Si cierta tecnología de spyware almacena y registra todos los datos y metadatos de un dispositivo sin ninguna capacidad de discriminación o limitación por parte del usuario, esto parece prima facie incompatible con los derechos humanos, ya que no habría capacidad operativa para el tipo de limitación requerida para el cumplimiento con derechos humanos.[52]

Por lo tanto, **cuando las medidas 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 cuales en ningún momento se verán involucradas en la comisión de hechos delictivos, **será notorio que existen medidas menos lesivas para conseguir la finalidad perseguida.**

Dentro de las medidas menos lesivas y más efectivas encontramos la prevención primaria o social, que atiende a investigar y comprender el fenómeno delictivo desde sus orígenes para poder evitarlo desde la raíz, así como medidas focalizadas únicamente respecto de personas cuya relevancia para una investigación puede ser demostrada con algún elemento de prueba.

D. Estudio de proporcionalidad en estricto sentido de la medida

La última grada de este método de adjudicación consiste en efectuar un balance o ponderación entre dos principios que compiten en un caso concreto. Dicho análisis requiere comparar el grado de intervención en el derecho fundamental que supone la medida legislativa examinada frente al grado de realización del fin perseguido por esta.[53] Las decisiones sobre la vigilancia de las comunicaciones deben considerar la sensibilidad de la información accesible y la gravedad de la infracción sobre los derechos humanos y otros intereses en competencia.

Para lo anterior, es importante destacar que las tecnologías de vigilancia de comunicaciones interfieren de manera intensa con distintos derechos humanos, como lo son el derecho a la privacidad, protección de datos personales y libertad de expresión. Por tanto, la vigilancia de las comunicaciones debería ser considerada como un acto altamente intrusivo que interfiere con los derechos humanos, amenazando los cimientos de una sociedad democrática.

---

52. Relatora Especial sobre la Lucha contra el Terrorismo, Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach, abril 2023, pár. 44, pp. 37-38. Menciona que el anterior Relator Especial sobre la libertad de opinión y de expresión consideró que la falta de pruebas convincentes de que el uso de tecnologías de spyware pueda restringirse técnicamente a fines lícitos justificaba una moratoria en: A/HRC/41/35,pár. 49.

53. Primera Sala de la Suprema Corte de Justicia de la Nación, Amparo en revisión 237/ 2014, Ponente: Arturo Zaldívar Lelo de Larrea, aprobado por mayoría de votos. De esta sentencia se emitió la Tesis Aislada CCLXX/2016 (10a.) "TERCERA ETAPA DEL TEST DE PROPORCIONALIDAD. EXAMEN DE LA NECESIDAD DE LA MEDIDA LEGISLATIVA." Registro: 2013154

El grado de afectación se potencializa frente al hecho –mencionado con anterioridad– de que las medidas de vigilancia tienden a implicar la recolección masiva e indiscriminada de información de millones de personas; la inmensa mayoría de las cuales, nunca se verán involucradas en la investigación de hecho delictivo alguno. Usar herramientas de vigilancia de las comunicaciones para fines de prevención del delito es, entonces, sumamente problemático porque deriva en que ningún crimen se ha cometido y se está realizando un acto de molestia sobre ciudadanas que no están sujetas a ningún proceso penal.[54] Asimismo, la información que se retiene suele ser excesiva en comparación con la amenaza que se está buscando combatir.

De acuerdo con la jurisprudencia y doctrina constitucional e internacional en materia de derechos humanos, se ha entendido que 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[55]; y ***proporcional*** si la afectación al derecho humano no resulta exagerada o desmedida frente a las ventajas que se obtienen mediante tal limitación.[56]

De esta manera, las injerencias en el derecho a la privacidad únicamente son permisibles en circunstancias limitadas, cuando no solo persiguen una finalidad legítima,[57] sino que son estrictamente necesarias y proporcionadas en sus efectos. En dicha línea, el CDH ha señalado que no basta con que las medidas restrictivas de derechos se utilicen para conseguir fines permisibles, sino que también deben ser necesarias y ajustarse al principio de proporcionalidad, en el sentido de que *"deben ser adecuadas para desempeñar su función protectora; debe ser el instrumento menos perturbador de los que permitan conseguir el resultado deseado, y deben guardar proporción con el interés que debe protegerse"*.[58]

Consecuentemente, en atención a los principios de necesidad y proporcionalidad, las medidas de vigilancia solamente 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 por la vigilancia.

---

54. SURVEILLE. "Surveillance: Ethical Issues, Legal Limitations,and Efficiency", 4 de Julio del 2015, disponible en: https://surveille.eui.eu/wp-content/uploads/sites/19/2015/04/D4.10-Synthesis-report-from-WP4.pdf p. 22

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

56. Ibidem, párr. 83

57. A pesar de que el artículo 17 del PIDCP no establece expresamente que las injerencias puedan justificarse sobre la base de una finalidad legítima, tanto el Comité de Derechos Humanos como los tribunales regionales de derechos humanos han interpretado que esa limitación se encuentra implícita en el alcance del derecho. Véanse, por ejemplo: CDH, Van Hulst vs. Países Bajos, UN Doc. CCPR/C/82/D/903/1999 (2004), pp. 7.6-7.10; y Weber y Saravia vs. Alemania (App No. 54934/00), Decisión de 29 de junio de 2006, pp. 103-137.

58. Comité de Derechos Humanos, Comentario General 27 [al analizar el derecho a la libertad de circulación bajo el PIDCP, Art. 12], UN Doc. CCPR/C/21/Rev.1/Add/9 (1999), pár. 1; y Comentario General 34, UN Doc. CCPR/C/GC/34 (2011), pár. 34.

En esta línea, el TEDH ha resaltado en su jurisprudencia reiterada que la existencia de salvaguardas adecuadas y efectivas resulta determinante para el análisis respecto de la necesidad y proporcionalidad de legislaciones que facultan invasiones a la privacidad.[59]

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,[60] el Relator Especial de la ONU para el Derecho a la Libertad de Expresión y Opinión,[61] la Alta Comisionada para los Derechos Humanos de la ONU,[62] la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana sobre Derechos Humanos,[63] 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.[64]

59. TEDH, Caso de la Asociación para la Integración Europea y los Derechos Humanos y Ekimdzhiev vs. Bulgaria, Aplicación No. 62540/00, Sentencia de 28 de Junio de 2007; Caso Weber y Sarabia vs. Alemania, Aplicación No. 54934/00, Decisión de 29 de Junio de 2006.

60. Asamblea General de la Organización de las Naciones Unidas, Resolución A/RES/68/167 sobre el derecho a la privacidad en la era digital, 18 de Diciembre de 2013.

61. ONU. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de expresión Frank La Rue, 17 de abril de 2013, A/HRC/23/40, párr. 81:
"La legislación debe estipular que la vigilancia estatal de las comunicaciones debe ocurrir únicamente bajo las circunstancias más excepcionales y exclusivamente bajo la supervisión de una autoridad judicial independiente. Salvaguardas deben ser articuladas en la ley en relación a la naturaleza, alcance y duración de las posibles medidas, los motivos necesarios para ordenarlas, las autoridades competentes para autorizar, llevar a cabo y supervisarlas, y el tipo de recursos previstos en la ley para obtener una reparación". (traducción propia)

62. OACNUDH, El derecho a la privacidad en la era digital, 30 de Junio de 2014, A/HRC/27/37, párr. 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. La "protección de la ley" debe ser otorgada a través de salvaguardas procesales efectivas, incluyendo arreglos institucionales efectivos y financiados adecuadamente. Es claro, sin embargo, que la falta de supervisión efectiva ha contribuido a una falta de rendición de cuentas por intrusiones arbitrarias o ilegales en el derecho a la privacidad en el entorno digital. 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)

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

64. Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://necessaryandproportionate.org/es/13-principles/

E. Salvaguardas

a. 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 de medidas de vigilancia encubierta que invaden la privacidad de las personas ha sido resaltada por la Relatoría Especial para la Libertad de Expresión de la CIDH, la cual ha señalado que (énfasis añadido):

> *Las decisiones de realizar tareas de vigilancia que invadan la privacidad de las personas d**eben 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.*[65]

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'"*, entendiéndose como los siguientes métodos de obtención de información (énfasis añadido):[66]

> *En todo caso, la efectiva protección de los derechos a la vida privada y a la libertad de pensamiento y de expresión, sumado al extremo riesgo de arbitrariedad que supone la utilización de las técnicas de vigilancia, selectiva o a gran escala, de las comunicaciones, máxime ante las nuevas tecnologías existentes, determinan para esta Corte que **cualquier medida en tal sentido (lo que incluye la interceptación, vigilancia y seguimiento de todo tipo de comunicación, sea telefónica, telemática o por otras redes exige que sea una autoridad judicial la que decida sobre su procedencia, definiendo a su vez los límites que se imponen, incluidos el modo, tiempo y alcances de la medida autorizada**.*
>
> *Asimismo, dado su carácter invasivo en la vida privada de las personas y ante la exigencia de establecer controles especialmente rigurosos, **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 privadas** que, por distintos motivos, lícitamente la administren o gestionen, requieren también de autorización judicial.*
>
> *Así las cosas, el Tribunal Interamericano es consciente de que el derecho a la privacidad demanda medidas de protección en torno al uso de las nuevas tecnologías, incluido el internet, en el marco de las actividades de inteligencia. En consecuencia, **se requiere igualmente autorización judicial previa para el empleo de técnicas de vigilancia y seguimiento con relación a personas determinadas que impli-***

65. 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.

66. 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, párrs. 542, 547, 551 y 553.

quen el acceso a bases de datos y sistemas de información no públicos que almacenen y procesen datos personales, el rastreo de usuarios en la red informática o la localización de dispositivos electrónicos.[67]

De igual forma, refuerza la noción de protección especial que requiere la información obtenida y clasificada como ***"datos sensibles"***, en el sentido siguiente (énfasis añadido):

> ***La exigencia de autorización judicial previa en estos ámbitos se sustenta, además, en la necesidad de brindar una protección reforzada a los datos sensibles de las personas****, entendidos como una categoría "más estrecha" de datos personales [...] que abarca aquellos que afectan "a los aspectos más íntimos de las personas", y que, según el contexto cultural, social o político, podría incluir, entre otros, "datos relacionados con la salud personal, las preferencias sexuales o vida sexual, las creencias religiosas, filosóficas o morales, la afiliación sindical, los datos genéticos, los datos biométricos dirigidos a identificar de manera unívoca a una persona física, las opiniones políticas o el origen racial o étnico, información sobre cuentas bancarias,documentos oficiales, información recopilada de niños y niñas o geolocalización personal".*[68] *En definitiva, se trata de datos que* ***merecen una protección especial porque permiten calificar al individuo y ofrecen sustento para la elaboración de perfiles personales.***
>
> *El Tribunal destaca que la necesaria intervención de una autoridad judicial en todos estos ámbitos es coherente con el rol de garantes de los derechos humanos que corresponde a las juezas y los jueces en un sistema democrático, cuya necesaria independencia posibilita el ejercicio de un control objetivo, conforme a Derecho, respecto del actuar de los otros órganos del poder público, en este caso, de los servicios de inteligencia del Estado.* ***Para el efecto, la autoridad judicial será la encargada de evaluar, en las circunstancias del caso concreto, el cumplimiento de las exigencias previamente descritas y de llevar a cabo el juicio de proporcionalidad con relación a la medida solicitada.***
>
> *Así, en congruencia con la jurisprudencia interamericana, la resolución que dicte la autoridad judicial habrá de estar debidamente motivada, pues, de lo contrario, sería una decisión arbitraria.* ***Por consiguiente, la resolución judicial deberá demostrar, mediante una argumentación racional, que han sido ponderados todos los requisitos constitucionales, legales y convencionales, así como los otros elementos que justifiquen, según corresponda, la concesión o la negativa de la medida.***

---

67. ONU, Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, A/HRC/23/40, párr. 86; Informe de OACNUDH, "El derecho a la privacidad en la era digital", A/HRC/27/37, párr. 45; Comité de Derechos Humanos, Observaciones finales sobre el cuarto informe periódico de la República de Corea, U.N. Doc. CCPR/C/COR/CO/4, 3 de diciembre de 2015, párr. 43; y Consejo de Derechos Humanos, Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, U.N. Doc. A/HRC/35/22, 30 de marzo de 2017, párrs. 19 y 78. Véase también, Tribunal de Justicia de la Unión Europea, Casos Tele2 Sverige AB Vs. Post-och telestyrelsen, y Secretary of State for the Home Department Vs. Tom Watson y otros, No. C-203/15 y C-698/15, Sentencia de 21 de diciembre de 2016, párr. 120.

68. Principios Actualizados del Comité Jurídico Interamericano sobre la Privacidad y la Protección de Datos Personales, con Anotaciones, Principio 9 y pág. 24. También véase, Identidad de género, e igualdad y no discriminacióna parejas del mismo sexo. Obligaciones estatales en relación con el cambio de nombre, la identidad de género, y los derechos derivados de un vínculo entre parejas del mismo sexo (interpretación y alcance de los artículos 1.1, 3, 7, 11.2, 13, 17, 18 y 24, en relación con el artículo 1 de la Convención Americana sobre DerechosHumanos). Opinión Consultiva OC-24/17 de 24 de noviembre de 2017. Serie A No. 24, párr. 136, y Consejo de Europa, Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, 28 de enero de 1981, artículo 6.

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

b. Supervisión independiente

La Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana ha señalado que *"los Estados deben establecer mecanismos de supervisión independientes sobre las autoridades encargadas de realizar las tareas de vigilancia"*.[69]

En igual sentido, en la referida resolución *"El derecho a la privacidad en la era digital"*, se recomienda 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"*.[70]

Por su parte, el Relator Especial sobre el derecho a la libertad de opinión y expresión de la ONU ha expresado que:

> *Los Estados deben ser completamente transparentes respecto del uso y alcance de los poderes y técnicas de vigilancia de las comunicaciones. Deben publicar, como mínimo, información agregada sobre el número de solicitudes aprobadas y rechazadas, una desagregación de las solicitudes por proveedor de servicios y por investigación y propósito.*
>
> *Los Estados deben otorgar a los individuos suficiente información para permitirles comprender totalmente el alcance, naturaleza y aplicación de leyes que permiten la vigilancia de comunicaciones. Los Estados deben permitir a los proveedores de servicios la publicación de los procedimientos que aplican para manejar la vigilancia de comunicaciones estatal, adherirse a esos procedimientos, y publicar registros sobre la vigilancia de comunicaciones estatal. (...).*[71]

De igual forma, la Corte IDH ha indicado en el referido caso CAJAR en cuanto a la supervisión de las actividades de inteligencia lo siguiente (énfasis añadido):

> *564. En cuanto a la supervisión de las actividades de inteligencia, se hace necesario que el marco jurídico establezca, sin perjuicio del control judicial sobre medidas o acciones específicas en situaciones concretas, una institución civil independiente de los servicios de inteligencia y del*

---

69. CIDH, Relatoría Especial para la Libertad de Expresión, Libertad de Expresión e Internet, 31 de diciembre de 2013, OEA/Ser.L/V/II, párr. 170

70. ONU, Asamblea General, Resolución aprobada por la Asamblea General el 18 de diciembre de 2013, 68/167, "El derecho a la privacidad en la era digital", A/RES/68/167, 21 de enero de 2014.

71. ONU, Informe del Relator Especial sobre el derecho a la libertad de opinión y expresión de la Organización de las Naciones Unidas, 17 de abril de 2013, A/HRC/23/40.

> *Poder Ejecutivo, de naturaleza parlamentaria, administrativa o jurisdiccional, la cual, además de contar con los conocimientos técnicos sobre la materia, debe estar dotada de las facultades para ejercer sus funciones, incluido el acceso directo y completo a la información y los datos indispensables para cumplir su cometido. El mandato de esta institución civil de supervisión debe abarcar la fiscalización en torno a los siguientes aspectos: a) el acatamiento, por parte de los servicios de inteligencia, de las disposiciones legales que rigen su actuación y de los instrumentos sobre derechos humanos; b) la eficiencia y eficacia de sus actividades, evaluando su rendimiento; c) su situación financiera y presupuestaria, y la administración de sus fondos, y, d) sus métodos y prácticas administrativas.*

Algunos ejemplos de este tipo de mecanismos incluyen al *Investigatory Powers Commissioner Office* en el Reino Unido,[72] la *Office of the Intelligence Commissioner* de Canadá[73] o la *Privacy and Civil Liberties Oversight Board* de los Estados Unidos,[74] las cuales poseen facultades para acceder y revisar cualquier información relacionada a medidas de vigilancia encubierta y rendir informes periódicos respecto de sus hallazgos.

De igual forma, la Corte IDH refiere la importancia de establecer mecanismos a nivel internacional *"para que quienes se consideren afectados por actividades arbitrarias de inteligencia puedan obtener una reparación efectiva, incluida la compensación por los daños que se hayan provocado".*[75]

c. Derecho de notificación

Otra de las salvaguardas fundamentales para proteger el derecho a la vida privada, garantizar el debido proceso y el acceso a un recurso efectivo frente a potenciales abusos de las medidas de vigilancia es el derecho de notificación a la persona afectada. Es decir, 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.

---

72. Investigatory Powers Commissioner's Office, disponible en: https://www.ipco.org.uk/

73. Office of the Intelligence Commissioner, disponible en: https://www.canada.ca/en/intelligence-commissioner.html

74. U.S. Privacy and Civil Liberties Oversight Board, disponible en: https://www.pclob.gov/Board/Index

75. 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. 565.

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 (énfasis añadido):

> ***Los individuos deben contar con el derecho a ser notificados que han sido sujetos de medidas de vigilancia*** *de sus comunicaciones o que sus comunicaciones han sido accesadas por el Estado. Reconociendo que la notificación previa o concurrente puede poner en riesgo la efectividad de la vigilancia, los individuos deben ser notificados, 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.*[76]

El derecho de notificación ha sido reconocido, además, por el 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.[77]

Finalmente, existen otros instrumentos de carácter internacional referentes al control de medidas de vigilancia en términos generales que vale la pena enunciar:

a) ***Principios de Johannesburgo sobre la Seguridad Nacional, la Libertad de Expresión y el Acceso a la Información*** (en adelante *"Principios de Johannesburgo"*) — elaborados en 1995 por un grupo de expertos en derecho Internacional, seguridad y derechos humanos.

Al respecto, el Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión ha señalado que dichos Principios *"ofrecen una guía útil para evaluar las demandas a menudo contrapuestas de libertad de expresión y seguridad nacional"*.[78]

b) ***Principios Globales sobre Seguridad Nacional y el Derecho a la Información***, conocidos como ***"Principios de Tshwane"*** (en adelante *"Principios de Tshwane"*) — redactados en 2013 por 22 organizaciones y centros académicos, con la asesoría de más de 500 expertos procedentes de más de 70 Estados, incluidos Relatores Especiales de las Naciones Unidas y de los sistemas regionales de derechos humanos.

---

76. *Ídem*.

77. TEDH, Caso de la Asociación para la Integración Europea y los Derechos Humanos y *Ekimdzhiev vs. Bulgaria*, Aplicación No. 62540/00, Sentencia de 28 de junio de 2007.

78. Comisión de Derechos Humanos, Informe del Relator Especial, Sr. Abid Hussain, U.N. Doc. E/CN.4/1996/39, 22 de marzo de 1996, párr. 4. El informe del Relator Especial, el cual incluye como anexo los Principios de Johannesburgo, se encuentra disponible en: https://undocs.org/Home/Mobile?FinalSymbol=E%2FCN.4%2F1996%2F39&Language=E&DeviceType=Desktop&LangRequested=False

El Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión ha indicado que estos Principios *"ofrecen orientación a los Estados que procuran equilibrar sus intereses al proteger información y asegurar el derecho de la sociedad a la información".*[79]

79. Asamblea General de las Naciones Unidas, Nota del Secretario General, Informe del Relator Especial sobre la Libertad de Opinión y Expresión, Sr David Kaye, U.N. Doc. A/70/361, 8 de septiembre de 2015, párr. 44. Los Principios se encuentran disponibles en: https://www.oas.org/es/sla/ddi/docs/acceso_informacion_Taller_Alto_Nivel_Paraguay_2018_documentos_referencia_Principios_Tshwane.pdf

CAPÍTULO DOS

Normas que regulan la vigilancia de comunicaciones en México

En México, el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos[80] 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, México es parte de la Convención Americana sobre Derechos Humanos (CADH) y el Pacto Internacional de Derechos Civiles y Políticos (PIDCP) que reconocen en sus artículos 11 y 17 respectivamente, el derecho a la vida privada, las cuáles se consideran parte del parámetro de regularidad constitucional por virtud del artículo 1° de la Constitución.

Así mismo, 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 al establecer que:

> ***Las comunicaciones privadas son inviolables.*** *La ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley.*
>
> ***Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada.*** *Para ello, la autoridad competente deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de*

80. Constitución Política de los Estados Unidos Mexicanos. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

la misma y su duración. La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor. [...].

De esta manera, desde el texto constitucional se establecen algunas directrices respecto de quién, cómo y cuándo puede llevar a cabo medidas de vigilancia de comunicaciones. A continuación se sintetizan los aspectos más relevantes de la regulación de estas medidas.

I. ¿Quién puede llevar a cabo medidas de vigilancia de comunicaciones?

El artículo 16 constitucional establece dos categorías de autoridades competentes para llevar a cabo medidas de vigilancia de comunicaciones como la intervención de comunicaciones privadas: autoridades federales facultadas por una ley y el Ministerio Público de las entidades federativas.

Con base en lo anterior, las autoridades facultadas para llevar a cabo medidas de vigilancia de comunicaciones son:

a) La Guardia Nacional, facultada por la Ley de la Guardia Nacional (LGN);[81]

b) El Centro Nacional de Inteligencia (CNI), facultado por la Ley de Seguridad Nacional (LSN);[82]

c) La Fiscalía General de la República, facultada por el Código Nacional de Procedimientos Penales (CNPP),[83] incluyendo a la Unidad del Cuerpo Técnico de Control de la Fiscalía Especializada en Materia de Delincuencia Organizada (FEMDO) de la FGR, facultada por la Ley Federal contra la Delincuencia Organizada;[84]

d) Las Fiscalías de las 32 entidades federativas, facultadas por el CNPP; y

e) La Fiscalía General de Justicia Militar, facultada por el Código Militar de Procedimientos Penales (CMPP).[85]

---

81. Ley de la Guardia Nacional. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGN.pdf

82. Ley de Seguridad Nacional. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LSN.pdf

83. Código Nacional de Procedimientos Penales. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP.pdf

84. Ley Federal contra la Delincuencia Organizada. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFCDO.pdf

85. Código Militar de Procedimientos Penales. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/CMPP.pdf

Algunas otras autoridades federales y órganos autónomos como la Secretaría de Hacienda y Crédito Público (SHCP), la Comisión Federal de Competencia (COFECE), la Auditoría Superior de la Federación (ASF) y el Instituto Nacional Electoral (INE) han pretendido derivar facultades de vigilancia de comunicaciones a partir de facultades genéricas de acceso a la información en posesión de particulares, como parte de sus facultades para llevar a cabo investigaciones en el marco de sus competencias. Sin embargo, dichas interpretaciones son de una legalidad y constitucionalidad dudosa, máxime si las mismas no se adhieren al requisito constitucional de autorización judicial federal.

II. ¿Qué formas de vigilancia de comunicaciones son reconocidas por la Ley en México?

A. Intervención de comunicaciones privadas

La intervención de comunicaciones privadas es definida por el artículo 291 del CNPP de la siguiente manera:

> *La intervención de comunicaciones privadas, abarca todo sistema de comunicación, o programas que sean resultado de la evolución tecnológica, que permitan el intercambio de datos, informaciones, audio, video, mensajes, así como archivos electrónicos que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación, los cuales se pueden presentar en tiempo real.*

De manera similar en su contenido y alcance, los artículos 16 de la Ley Federal contra la Delincuencia Organizada (LFDO), 100 de la LGN, 34 de la LSN y 287 del CMPP mencionan a la intervención de comunicaciones privadas.

Resulta fundamental resaltar como tanto en su definición, como en diversos precedentes judiciales,[86] se reconoce una definición amplia del concepto de intervención de comunicaciones

86. SCJN. Segunda Sala. Tesis 2a. XXXV/2016 (10a.) COMUNICACIONES PRIVADAS. LA SOLICITUD DE ACCESO A LOS DATOS DE TRÁFICO RETENIDOS POR LOS CONCESIONARIOS, QUE REFIERE EL ARTÍCULO 190, FRACCIÓN II, DE LA LEY FEDERAL DE TELECOMUNICACIONES Y RADIODIFUSIÓN, DEBE REALIZARSE EN TÉRMINOS DEL ARTÍCULO 16 CONSTITUCIONAL Y SÓLO LA AUTORIDAD JUDICIAL PODRÁ AUTORIZAR LA ENTREGA DE LA INFORMACIÓN RESGUARDADA. Gaceta del Semanario Judicial de la Federación. Libro 32, Julio de 2016, Tomo I, página 776. Registro digital: 2011994; Plenos Regionales. Tesis PR.P.CN. J/23 P (11a.) DATOS CONSERVADOS POR LOS CONCESIONARIOS DE TELECOMUNICACIONES. SU ENTREGA A LA AUTORIDAD INVESTIGADORA REQUIERE AUTORIZACIÓN EXCLUSIVA POR PARTE DE LA AUTORIDAD JUDICIAL FEDERAL, DADO QUE CONSTITUYE UNA RESTRICCIÓN AL DERECHO HUMANO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS PREVISTO EN EL ARTÍCULO 16, DÉCIMO SEGUNDO PÁRRAFO, CONSTITUCIONAL. Gaceta del Semanario Judicial de la Federación. Libro 33, Enero de 2024, Tomo IV, página 3989. Registro digital: 2028011; y SCJN. Primera Sala. Tesis 1a. VI/2024 (11a.) DATOS CONSERVADOS POR LOS CONCESIONARIOS DE TELECOMUNICACIONES EN LAS DENOMINADAS "SÁBANAS DE LLAMADAS". EN TÉRMINOS DEL ARTÍCULO 16 CONSTITUCIONAL, ES COMPETENCIA EXCLUSIVA DE LOS JUECES FEDERALES AUTORIZAR A LA AUTORIDAD INVESTIGADORA EL ACCESO A ELLOS.. Gaceta del Semanario Judicial de la Federación. Libro 37, Mayo de 2024, Tomo II, página 2250. Registro digital: 2028870.

privadas en tanto comprende todo tipo de información y se entiende que comprende 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 registro, grabación, recolección y almacenamiento de la información, tanto en tiempo real como con posterioridad al momento en que se produce el proceso comunicativo.

B. La extracción de información de dispositivos electrónicos

Tanto el CNPP como el CMPP mencionan de manera explícita la posibilidad de llevar a cabo la "*extracción de información*", la cual consiste en "*la obtención de comunicaciones privadas, datos de identificación de las comunicaciones; así como 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*".

Si bien la conducta descrita encuadra en el concepto de intervención de comunicaciones privadas, dichas disposiciones optaron por explicitar que técnicas de investigación como la extracción de información de un dispositivo móvil o de un dispositivo o cuenta de almacenamiento en la nube también requieren el cumplimiento de los mismos requisitos establecidos por el artículo 16 constitucional.

C. La retención y acceso a datos conservados por empresas de telecomunicaciones

El artículo 190, fracción II, de la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR)[87] 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. Los *Lineamientos de Colaboración en Materia de Seguridad y Justicia*[88] (en adelante "*Lineamientos de Colaboración*"), emitidos

87. Ley Federal de Telecomunicaciones y Radiodifusión, disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR.pdf

88. Lineamientos de Colaboración en Materia de Seguridad y Justicia, disponibles en: https://www.ift.org.mx/sites/default/files/c-nspn-03-lcmsjmptfn.pdf

por el Instituto Federal de Telecomunicaciones (en adelante "IFT") establecen con mayor detalle las obligaciones de los concesionarios y autorizados respecto de la conservación y entrega de los datos de las comunicaciones de las personas usuarias de servicios de telecomunicaciones.

El artículo 303 del CNPP faculta a la FGR y las fiscalías de las entidades federativas a acceder a dicho registro, así como a información conservada por proveedores de aplicaciones y servicios, sin definir con precisión a qué proveedores se refiere.

Por su parte, el artículo 9, fracción XXVI, de la LGN faculta a la Guardia Nacional a solicitar *"la información con que cuenten"* concesionarios, permisionarios, operadoras telefónicas y todas aquellas comercializadoras de servicios en materia de telecomunicaciones o de sistemas de comunicación vía satélite.

D. La geolocalización en tiempo real de equipos de comunicación

Los artículos 3, fracción XXXV y 190, fracción I de la LFTR establecen la figura de la localización geográfica en tiempo real de dispositivos de telefonía móvil, la cual consiste en *"la ubicación aproximada en el momento en que se procesa una búsqueda de un equipo terminal móvil asociado a una línea telefónica determinada".*

Esta medida de vigilancia se encuentra contemplada en el artículo 303 del CNPP, respecto de la FGR y las fiscalías de las entidades federativas, así como por la Fiscalía Especial en Investigación de los Delitos de Desaparición Forzada de la propia FGR. Asímismo, el artículo 9, fracción XXVI de la LGN, contempla esta medida respecto de la Guardia Nacional.

E. Recolección, almacenamiento y entrega de datos de geolocalización de personas usuarias de servicios financieros

Las Disposiciones de carácter general a que se refiere el artículo 115 de la Ley de Instituciones de Crédito,[89] obligan a las instituciones de crédito a recabar datos de geolocalización de los dispositivos a través de los cuáles un cliente de dichas instituciones realice operaciones, actividades o servicios de forma no presencial.

Dichas disposiciones administrativas emitidas por la Secretaría de Hacienda y Crédito Público (SHCP) obligan al almacenamiento indiscriminado de los datos de geolocalización por un pe-

89. Secretaría de Hacienda y Crédito Público, Disposiciones de carácter general a que se refiere el artículo 115 de la Ley de Instituciones de Crédito, disponible en: https://www.gob.mx/cms/uploads/attachment/file/709513/DCG_Compiladas_Instituciones_de_Credito_08.03.2022.pdf

riodo de tiempo indeterminado "*no menor a diez años*", según la disposición 59 de dicha norma. A su vez, la disposición 54 establece la obligación de transferir los datos de geolocalización almacenados a autoridades definidas con poca claridad, sin requerir autorización judicial previa y sin ninguna otra salvaguarda o medidas de rendición de cuentas susceptibles de inhibir el uso indebido de la información.

F. Monitoreo de la red pública de Internet

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.

III. ¿En qué casos y bajo qué procedimientos pueden llevarse a cabo medidas de vigilancia de comunicaciones en México?

A. Requisitos de procedencia material

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. Además, prohíbe su procedencia en las materias electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor.

Por su parte, la Ley General de Protección de Datos en Posesión de Sujetos Obligados (LGPDPSO)[90] exige en su artículo 80 *"la obtención y tratamiento de datos personales (...) por parte de las sujetos obligados competentes en instancias de seguridad, procuración y administración de justicia, está limitada a aquellos supuestos y categorías de datos que resulten necesarios y proporcionales para el ejercicio de las funciones en materia de seguridad nacional, seguridad pública, o para la prevención o persecución de los delitos".*

90. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

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.

En el caso del CNPP, el artículo 291 establece que la procedencia de la solicitud de autorización para la intervención de comunicaciones privadas requiere únicamente 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. Aun cuando podría desprenderse del requisito de motivación que el juez de control debe sustentarse en indicios que le permitan valorar si existe dicha necesidad, la redacción de dicho artículo podría ser más explícita en establecer un estándar probatorio de necesidad o "*causa probable*", como el que existe en otras jurisdicciones, como la estadounidense.

Por su parte, la LGN sí establece un estándar de necesidad para las medidas de vigilancia de comunicaciones en su artículo 100, al establecer el requisito de que se constate *"la existencia de indicios suficientes que acrediten que se está organizando la comisión de delitos"* enlistados en el artículo 103 de la LGN. Por lo que, en teoría, la medida de vigilancia para fines de prevención del delito no debería autorizarse en cualquier caso, sino solo en aquéllos en los que la Guardia Nacional aporte indicios suficientes para acreditar que la comisión de uno de los delitos enlistados se encuentra en vía de ser materializado.

En el caso de la LSN, el estándar de necesidad resulta ambiguo, pues, si bien en su artículo 33 parece requerir el cumplimiento del requisito de *"inminencia"* de las amenazas a la seguridad nacional descritas en el artículo 5 de dicha Ley, en su artículo 35 parece requerir únicamente encontrarse *"en los supuestos a los que se refiere el artículo 5 de la (...) Ley"*, cuya redacción es amplia y ambigua.

Respecto de otras medidas de vigilancia, como el acceso a datos conservados o la geolocalización en tiempo real, el CNPP faculta a las fiscalías a solicitar autorización cuando *"el Ministerio Público considere necesaria"* la práctica de dichas medidas para obtener información asociada a una línea *"que se encuentra relacionada con los hechos que se investigan"*, lo cual otorga una gran discrecionalidad. A su vez, la LGN permite a la Guardia Nacional solicitar la geolocalización de dispositivos de manera genérica *"para el cumplimiento de sus fines de prevención de los delitos"*.

En los casos que disponen la recolección y conservación de datos de personas usuarias de servicios de telecomunicaciones o de servicios financieros, dicha recolección y conservación es masiva e indiscriminada, en tanto basta ser usuaria de dichos servicios para que se lleve a cabo dicha recolección y almacenamiento. Además, como previamente fue mencionado, en el

caso de los datos de geolocalización conservados por instituciones de crédito, las normas no definen con claridad los supuestos materiales en los que dicha información debe ser entregada a autoridades que la requieran.

B. Control judicial

El artículo 16 constitucional establece con claridad la necesidad de una autorización judicial federal para llevar a cabo la intervención de comunicaciones privadas. El CNPP,[91] la LGN[92] y la LSN[93] detallan el procedimiento a seguir, los requisitos de las solicitudes, los plazos y los elementos, modalidades y límites que debe establecer la resolución del juez de control federal que conozca de las solicitudes.

Respecto de la entrega de datos conservados por empresas de telecomunicaciones y proveedores de contenidos, aplicaciones y servicios y la geolocalización en tiempo real, si bien la definición de *"intervención de comunicaciones privadas"* contempla tanto el contenido de las comunicaciones como los *"datos que identifiquen la comunicación"* o metadatos, ha existido incertidumbre e inconsistencias respecto de la necesidad de autorización judicial previa y respecto de si la competencia de los jueces de control federales para tramitar este tipo de solicitudes es exclusiva.

Aunque el artículo 303 del CNPP establece explícitamente desde 2016 que el acceso a datos conservados y la geolocalización en tiempo real debe estar precedida —como regla general— de una autorización judicial, el texto del artículo generó incertidumbre al establecer que dicha autorización debe solicitarse al *"juez de control del fuero correspondiente"*. Sin embargo, el Poder Judicial Federal ya ha establecido mediante jurisprudencia que es competencia exclusiva de los jueces de control federales el conocer de las solicitudes de acceso a datos conservados.[94]

No obstante que el Poder Judicial de la Federación ha entendido que los requisitos establecidos en el artículo 16 constitucional resultan aplicables a los metadatos de telecomunicaciones, el artículo 303 del CNPP establece excepciones a la regla del control judicial previo, estableciendo que *"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"*, las fiscalías pueden ordenar directamente la geolocalización en tiempo real o la entrega de datos conservados por parte de los concesionarios y proveedores.

---

91. CNPP. Artículos 292 a 302.

92. LGN. Artículos 100 a 106.

93. LSN. Artículos 33 a 48.

94. Plenos Regionales. Tesis PR.P.CN. J/23 P (11a.) Gaceta del Semanario Judicial de la Federación. Libro 33, Enero de 2024, Tomo IV, página 3989. Registro digital: 2028011; y SCJN. Primera Sala. Tesis 1a. VI/2024 (11a.) Gaceta del Semanario Judicial de la Federación. Libro 37, Mayo de 2024, Tomo II, página 2250. Registro digital: 2028870.

Cuando este mecanismo excepcional es utilizado por las fiscalías, el CNPP establece la obligación de informar al juez de control dentro de las 48 horas siguientes a que se haya cumplimentado el requerimiento, para efectos de que la autoridad judicial ratifique total o parcialmente la medida o revoque la misma.

Finalmente, aunque tanto el artículo 9, fracción XXVI, de la LGN, como el artículo 303 del CNPP establecen el requisito de autorización judicial federal previa —salvo las excepciones mencionadas— para la geolocalización en tiempo real y el acceso a datos conservados, 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.

C. Seguimiento y conclusión de las medidas

Tanto el CNPP, como la LGN y la LSN disponen la supervisión de las medidas por parte del juez de control. Por ejemplo, el artículo 294 del CNPP y 104 de la LGN establecen que el juez *"podrá en cualquier momento verificar que las intervenciones sean realizadas en los términos autorizados y, en caso de incumplimiento, decretar su revocación parcial o total".* En el caso de la LSN, el artículo 41 establece que *"el juez podrá requerir informes periódicos respecto de la ejecución de la autorización".*

Adicionalmente, la legislación establece varios supuestos en los que debe destruirse la información obtenida. El artículo 300 del CNPP contempla que la autoridad judicial ordenará la destrucción de los registros de intervención de comunicaciones privadas que no se relacionen con una conducta delictiva, salvo que la defensa de un imputado los considere útiles para su labor. También se dispone la destrucción cuando las intervenciones no hayan sido autorizadas o se rebasen los términos de la autorización judicial, así como cuando se decrete el archivo definitivo, el sobreseimiento o la absolución del imputado o en el caso de archivo temporal, cuando el delito prescriba.

En ningún caso se contempla la notificación a las personas afectadas por las medidas de vigilancia, las cuáles únicamente podrían tener conocimiento de las interferencias en su vida privada en el caso de que las mismas fueran utilizadas como prueba dentro de un procedimiento penal.

D. Registro

El artículo 16 de la Constitución establece que *"deberá existir un registro fehaciente de todas las comunicaciones entre jueces y Ministerio Público y demás autoridades competentes"* para solicitar medidas de vigilancia encubierta como la intervención de comunicaciones privadas, el acceso a datos conservados y la geolocalización en tiempo real.

Los artículos 297 y 298 del CNPP disponen la existencia de un registro de las intervenciones que debe contener las fechas de inicio y término de la intervención, un inventario pormenorizado de la información obtenida, la identificación de quienes hayan participado en los actos de investigación, entre otros datos. El registro debe ser numerado progresivamente y contener los datos de identificación necesarios.

El artículo 104 de la LGN ordena el levantamiento de un acta que contenga un inventario pormenorizado de la información obtenida durante la intervención y la entrega de un informe a la autoridad judicial que haya autorizado la medida. Por su parte, el artículo 37 de la LSN contempla el registro de las solicitudes de intervención de comunicaciones privadas en un libro de gobierno especial.

E. Transparencia

Las diversas normas que regulan las medidas de vigilancia suelen enfatizar la reserva de la información sobre las mismas, aduciendo la necesidad de secrecía para la consecución de los objetivos de prevención del delito, investigación del delito o la atención de amenazas a la seguridad nacional.

No obstante lo anterior, el Poder Judicial Federal ha establecido criterios que reconocen que, aún en dichos casos, no pueden establecerse reservas absolutas que eludan los principios de acceso a la información pública como el que requiere la realización de una prueba de daño.

En este sentido, en el Amparo en Revisión 105/2021, la Segunda Sala de la Suprema Corte de Justicia de la Nación (SCJN) realizó una interpretación sistemática del artículo 51 de la Ley de Seguridad Nacional con las disposiciones de la legislación especializada en materia de transparencia, para determinar lo siguiente (énfasis añadido):

> *54. Si un sujeto obligado pudiera simplemente invocar una causa legal de reserva sin llevar a cabo este ejercicio ponderativo, la mera vinculación de la información con alguno de estos dos conceptos en los términos que estableciera la ley conduciría indefectiblemente a su clasificación y, por ende, a la restricción del derecho de acceso a la información. Esto es básicamente lo que sucedería si se interpretara el artículo 51 de la Ley de Seguridad Nacional de manera aislada e independiente de las disposiciones legales especializadas en materia de transparencia. Bastaría con advertir una mínima relación de la información en posesión de la autoridad con alguno de los elementos que enuncia ese precepto legal para que el sujeto obligado la clasificara sin más como reservada por motivos de seguridad nacional.*
>
> *55. En cambio, de la interpretación sistemática del artículo 51 de la Ley de Seguridad Nacional con las diversas disposiciones de la Ley General y la Ley Federal que regulan* ***la prueba de daño se desprende que resulta indispensable realizar este ejercicio ponderativo antes de que el sujeto obligado pueda***

> ***clasificar información como reservada por motivos de seguridad nacional*** *con base en ese precepto legal. La razón para concluir esto también es muy sencilla. Mientras que en términos de la legislación especializada en materia de transparencia* ***la prueba de daño representa un elemento jurídico ineludible en la implementación de cualquier restricción legal del derecho de acceso a la información*** *por razones de orden público o seguridad nacional, el artículo 51 de la Ley de Seguridad Nacional obviamente entra en tal supuesto porque impone restricciones legales al ejercicio del derecho de acceso a la información específicamente por el segundo de estos motivos.*

Consecuentemente, la SCJN ha aclarado que la normativa de seguridad nacional debe interpretarse de manera conforme con la Constitución y no puede por sí sola justificar una reserva de información.[95] Por ello, previo a la reserva de información, la autoridad está obligada a realizar un ejercicio ponderativo de prueba de daño a través del cual se confirme de manera fundada y motivada que la causal de reserva efectivamente se actualiza en el caso concreto:[96]

> *60. Como se observa, interpretar el artículo 51 de la Ley de Seguridad Nacional sistemáticamente con las disposiciones de la legislación especializada en materia de transparencia desemboca en la aplicación de la prueba de daño respecto de la información relacionada con la generación de inteligencia para la seguridad nacional. También* ***da la posibilidad que se invoquen las excepciones por violaciones a derechos humanos o actos de corrupción a una reserva de información por motivos de seguridad nacional.*** *Por el contrario, de adoptarse una interpretación literal y aislada del precepto, se corre el riesgo de que dejen de aplicar los mecanismos jurídicos creados por el legislador justamente para darle el alcance que corresponde al derecho a la información y a la seguridad nacional en los distintos supuestos que se presenten en la práctica y, por consiguiente, de que se establezca a priori una prevalencia indebida de este fin constitucional sobre aquel derecho fundamental. Esto haría de las restricciones al derecho de acceso a la información por motivos de seguridad nacional la regla y no la excepción.*
> *61. Las anteriores consideraciones llevan a esta Segunda Sala a concluir que* ***el artículo 51 de la Ley de Seguridad Nacional debe interpretarse sistemáticamente con las disposiciones especializadas en materia de transparencia, en particular las que regulan la prueba de daño****. Al hacer que tengan aplicabilidad las normas relativas a dicho ejercicio ponderativo a cargo del sujeto obligado, esta postura interpretativa* ***maximiza el derecho de acceso a la información ante las reservas de información por motivos de seguridad nacional previstas en las leyes. Asimismo, abre la puerta a que se puedan oponer las excepciones por violaciones a derechos humanos, delitos de lesa humanidad o actos de corrupción previstas en los artículos 115 de la Ley General y 112 de la Ley Federal.*** *En esta tesitura, la interpretación sistemática del artículo impugnado resulta menos restrictiva para el derecho de acceso a la información que aquella que, atendiendo de forma exclusiva a su literalidad, simplemente excluye la aplicación de la prueba de daño y hace prevalecer la seguridad nacional en todos los casos en que exista una reserva legal por este motivo.*

---

95. Conforme a la fracción I del artículo 3 de la Ley de Seguridad Nacional (LSN), se entiende por Seguridad Nacional las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano, que conlleven a la protección de la nación mexicana frente a las amenazas y riesgos que enfrenta nuestro país.

96. Amparo en Revisión 105/2021, par. 42. Resuelto el veinticuatro de noviembre de dos mil veintiuno por la Segunda Sala de la Suprema Corte de Justicia de la Nación por unanimidad de cinco votos de los ministros Alberto Pérez Dayán, Luis María Aguilar Morales, José Fernando Franco González Salas, Javier Laynez Potisek (ponente) y Presidenta Yasmín Esquivel Mossa.

Adicionalmente, el marco jurídico mexicano contempla medidas de transparencia estadística al respecto de las medidas de vigilancia. Por ejemplo, el artículo 70, fracción XLVII, de la Ley General de Transparencia y Acceso a la Información Pública (en adelante, "LGTAIP") establece como obligación de transparencia oficiosa (énfasis añadido):

> *Artículo 70. En la Ley Federal y de las Entidades Federativas se contemplará que los sujetos obligados pongan a disposición del público y mantengan actualizada, en los respectivos medios electrónicos, de acuerdo con sus facultades, atribuciones, funciones u objeto social, según corresponda, la información, por lo menos, de los temas, documentos y políticas que a continuación se señalan:*
> *[...]*
> *XXX. Las estadísticas que generen en cumplimiento de sus facultades, competencias o funciones* ***con la mayor desagregación posible;***
> *[...]*
> *XLVII.* ***Para efectos estadísticos, el listado de solicitudes a las empresas concesionarias de telecomunicaciones y proveedores de servicios o aplicaciones de Internet para la intervención de comunicaciones privadas, el acceso al registro de comunicaciones y la localización geográfica en tiempo real de equipos de comunicación, que contenga exclusivamente el objeto, el alcance temporal y los fundamentos legales del requerimiento, así como, en su caso, la mención de que cuenta con la autorización judicial correspondiente,*** *y [...]*

No obstante lo anterior, en los Lineamientos Técnicos Generales,[97] emitidos por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) para reglamentar esta obligación, se excluyen datos estadísticos de las solicitudes que "*formen parte de una investigación en curso*", además de que excluyen al Consejo de la Judicatura Federal de la emisión de información estadística sobre medidas de vigilancia. Con estas disposiciones, la eficacia de la información estadística se ve gravemente disminuída en tanto no refleja el universo de solicitudes ni permite comparar la información para efectos de detectar anomalías entre lo reportado por autoridades requirentes y las autoridades que autorizan dichas medidas.

97. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Lineamientos técnicos generales para la publicación, homologación y estandarización de la información de las obligaciones establecidas en el título quinto y en la fracción IV del artículo 31 de la Ley General de Transparencia y Acceso a la Información Pública, que deben de difundir los sujetos obligados en los portales de Internet y en la Plataforma Nacional de Transparencia, disponibles en: https://snt.org.mx/wp-content/uploads/Lineamientos-Tecnicos-Generales-Version-Integrada.pdf

CAPÍTULO TRES

La vigilancia de comunicaciones en la práctica

I. Vigilancia en números oficiales

Las fuentes de información oficial sobre las técnicas de vigilancia establecidas en la ley mexicana son escasas. Actualmente, el Poder Judicial de la Federación publica algunas estadísticas sobre las técnicas de investigación resueltas por jueces federales y las autoridades facultadas para llevar a cabo técnicas como la intervención de comunicaciones privadas, el acceso a datos conservados y la geolocalización en tiempo real reportan —frecuentemente de forma incompleta— estadísticas sobre el número de solicitudes realizadas.

Durante los años 2016 y 2017 también existieron datos publicados por concesionarias y autorizadas en materia de telecomunicaciones. Sin embargo, el Instituto Federal de Telecomunicaciones (IFT) removió sin justificación la obligación de publicar dicha información.

A pesar de lo anterior, a continuación se presentan los datos oficiales, de los cuáles es posible desprender algunas tendencias e inconsistencias relevantes.

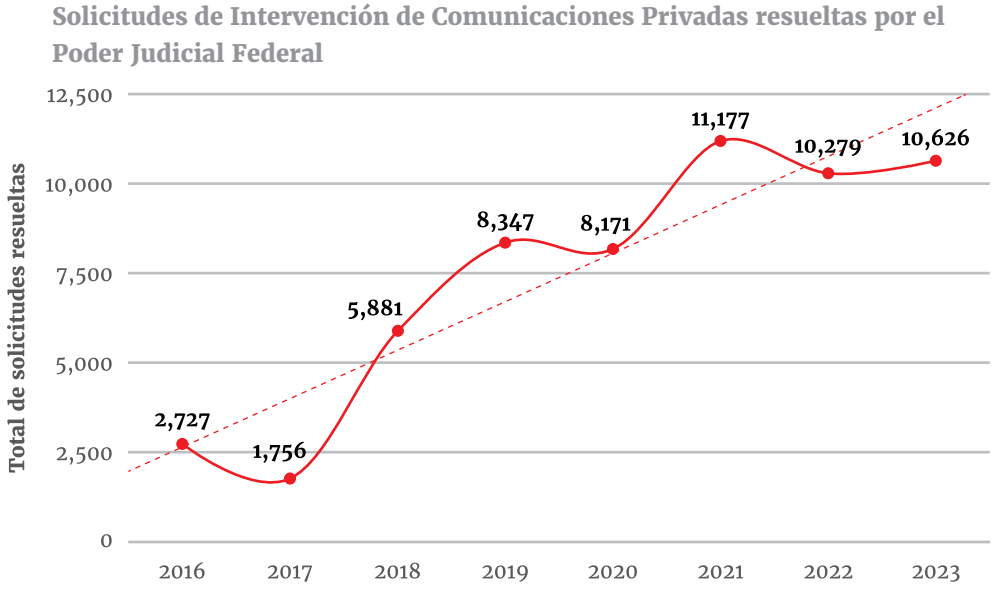
A. Intervención de comunicaciones privadas

Al consultar los datos publicados por autoridades federales en la Plataforma Nacional de Transparencia (en adelante "PNT"), se destaca que el Centro Nacional de Inteligencia (CNI) ha reportado en 0 el número de solicitudes de intervención de comunicaciones privadas desde el año 2016. La Fiscalía General de la República únicamente reporta datos desde 2020, al igual que la Guardia Nacional, creada en 2019.

	Guardia Nacional	Fiscalía General de la República
2020	92	552
2021	124	804
2022	96	869
2023	18	701

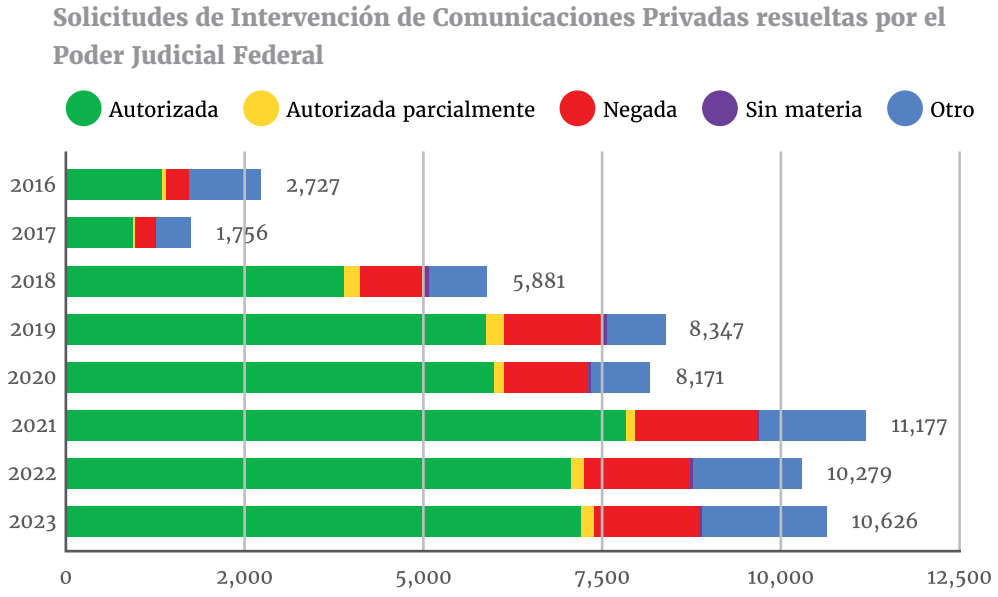
Tabla 3.1. *Plataforma Nacional de Transparencia. Solicitudes de Intervención de Comunicaciones Privadas.*

Por su parte, según datos publicados por el Poder Judicial de la Federación, existe una clara tendencia al alza en la resolución de solicitudes de intervención de comunicaciones privadas por parte de jueces federales en los últimos años.

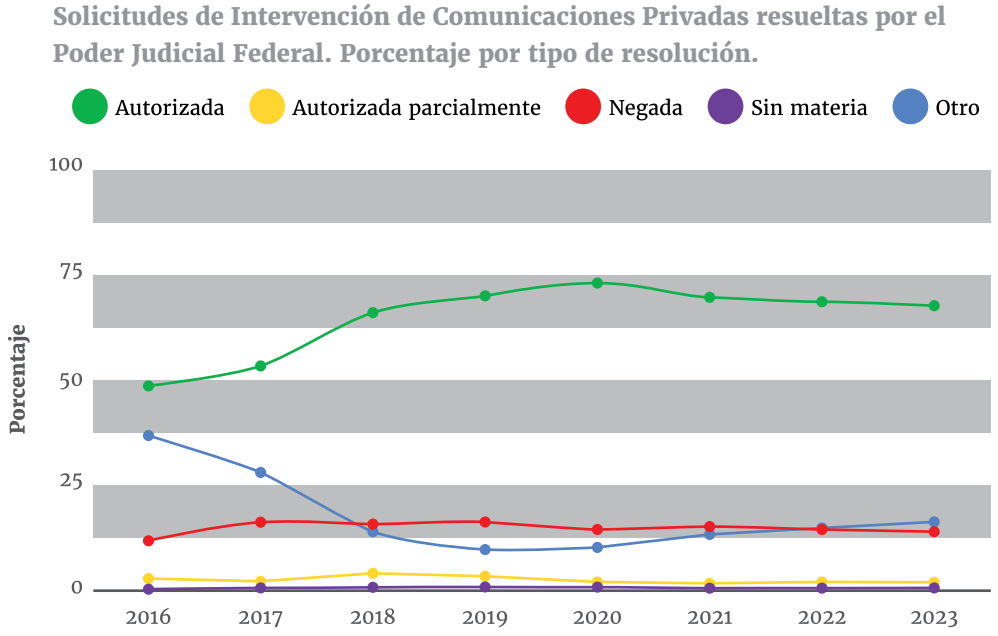


Gráfica 3.1. *CJF. Dirección General de Estadística Judicial. Anexos Estadísticos.*

Entre 2016 y 2023, en promedio el 67% de las solicitudes son autorizadas total o parcialmente, mientras que el 14.7% son negadas y el 17.8% tienen otro resultado no especificado.



Gráfica 3.2. *CJF. Dirección General de Estadística Judicial. Anexos Estadísticos.*



Gráfica 3.3. *CJF. Dirección General de Estadística Judicial. Anexos Estadísticos.*

Resulta importante advertir que el número de solicitudes de intervención de comunicaciones privadas reportado, no permite conocer el número de personas, dispositivos, cuentas o líneas afectadas, en tanto las autoridades suelen requerir autorización para llevar a cabo la intervención de comunicaciones privadas respecto de múltiples personas a través de una sola solicitud.

Por ejemplo, si bien la Guardia Nacional reportó haber solicitado la autorización para la intervención de comunicaciones privadas 92 veces en el año 2020. En respuesta[98] a una solicitud de acceso a la información realizada por R3D, la Guardia Nacional reportó haber intervenido las comunicaciones privadas de 289 líneas telefónicas (3.14 líneas por solicitud).

Adicionalmente, al consultar la PNT, se observa un amplio incumplimiento de la obligación de publicación de información estadística por parte de las fiscalías de las 32 entidades federativas, por lo que no resulta posible conocer el volumen de solicitudes llevadas a cabo por la mayoría de dichos entes. Aún en los casos en los que las fiscalías estatales sí han reportado información estadística, la información publicada no coincide con la información entregada a partir de solicitudes de acceso a la información realizadas por R3D.

Por ejemplo, en el año 2020, la Fiscalía General de Chihuahua reportó ante la PNT haber realizado 524 solicitudes de intervención de comunicaciones privadas. Sin embargo, en respuesta a una solicitud de acceso a la información, reportó haber realizado 601; misma situación se presenta en los casos de las Fiscalías del Estado de México, Guerrero y Sonora.

98. Guardia Nacional, Respuesta a la Solicitud de Información 2800100074421.

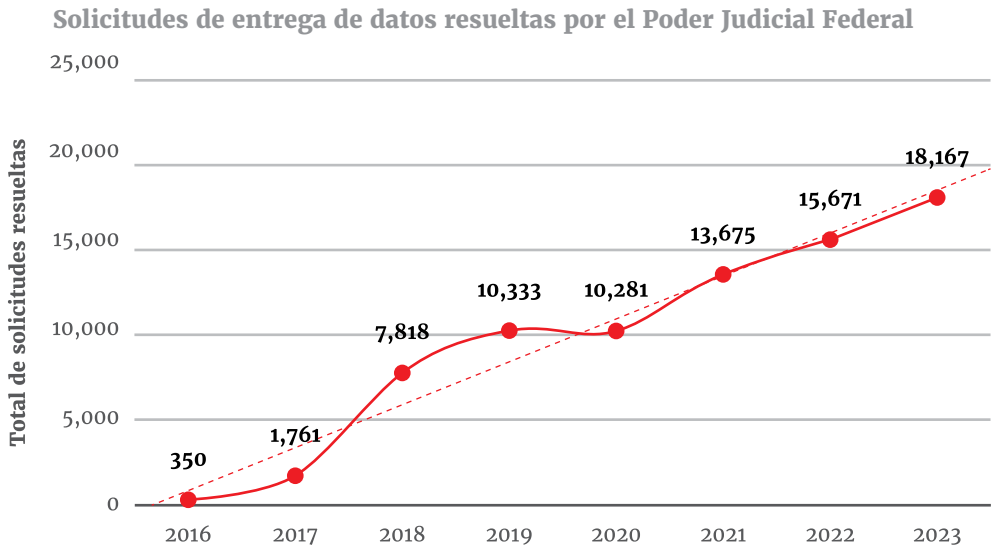
B. Acceso a Datos Conservados y Geolocalización en tiempo real

Al consultar los datos publicados por autoridades federales en la Plataforma Nacional de Transparencia, nuevamente el Centro Nacional de Inteligencia (CNI) ha reportado en cero (0) el número de solicitudes de intervención de comunicaciones privadas desde el año 2016. La Fiscalía General de la República únicamente reporta datos desde 2020, al igual que la Guardia Nacional, creada en 2019.

	Guardia Nacional	Fiscalía General de la República
2020	32	1967
2021	55	2017
2022	84	2299
2023	6	1891

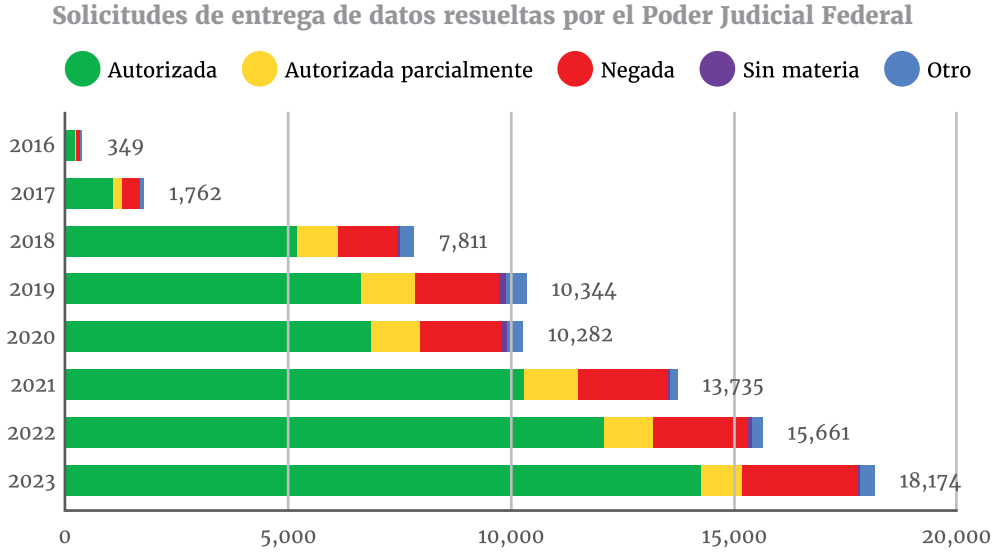
Tabla 3.2. *Plataforma Nacional de Transparencia. Solicitudes de Intervención de Comunicaciones Privadas.*

Por su parte, según datos publicados por el Poder Judicial de la Federación, también existe una clara tendencia al alza en la resolución de solicitudes de entrega de datos conservados por parte de jueces federales, especialmente a partir del año 2018:

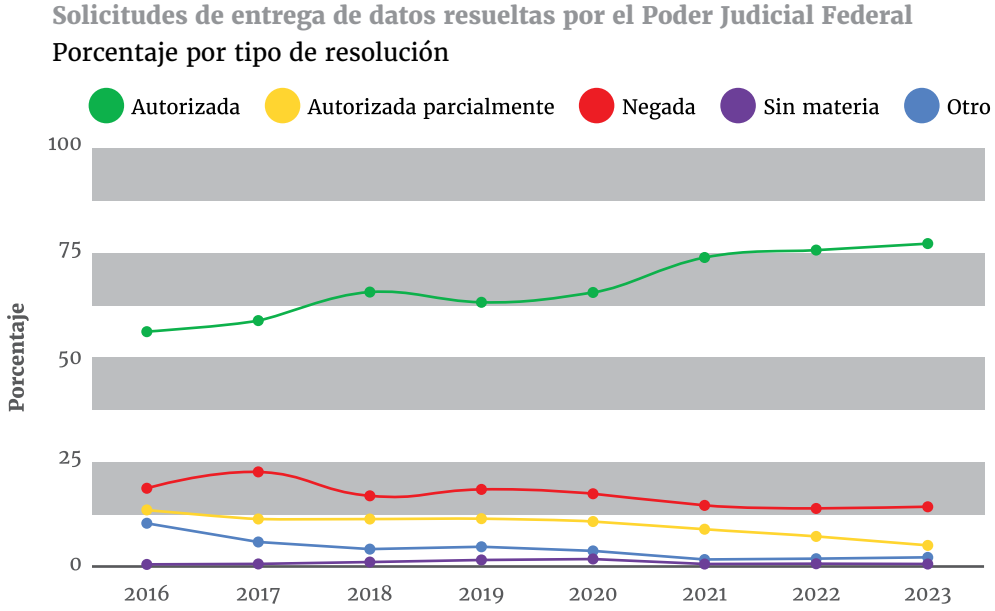


Gráfica 3.4. *CJF. Dirección General de Estadística Judicial. Anexos Estadísticos.*

Entre 2016 y 2023, en promedio el 78% de las solicitudes son autorizadas total o parcialmente, mientras que el 17.2% son negadas y el 4% tienen otro resultado no especificado.



Gráfica 3.5. *CJF. Dirección General de Estadística Judicial. Anexos Estadísticos.*



Gráfica 3.6. *CJF. Dirección General de Estadística Judicial. Anexos Estadísticos.*

Se reitera que el número de solicitudes de acceso a datos conservados y geolocalización reportados no permite conocer el número de personas y líneas afectadas, en tanto las autoridades suelen solicitar datos de múltiples personas a través de una sola solicitud.

Por ejemplo, si bien la Guardia Nacional reportó haber solicitado la autorización para el acceso a datos conservados 32 veces en el año 2020, en respuesta[99] a una solicitud de acceso a la información realizada por R3D, la Guardia Nacional reportó haber obtenido los datos de 66 líneas telefónicas (2 líneas por solicitud).

Como fue mencionado anteriormente, al consultar la PNT se observa un amplio incumplimiento de la obligación de publicación de información estadística por parte de las fiscalías de las 32 entidades federativas, por lo que no resulta posible conocer el volumen de solicitudes llevadas a cabo por la mayoría de dichos entes. Aún en los casos en los que las fiscalías estatales sí han reportado información estadística, la información publicada no coincide con la información entregada a partir de solicitudes de acceso a la información realizadas por R3D.

Por ejemplo, en el año 2020, las fiscalías del Estado de México, Guanajuato, Hidalgo y Tamaulipas reportaron ante la PNT haber realizado 1,728, 21, 3,988 y 1,578 solicitudes de acceso a datos conservados y geolocalización, respectivamente. En contraste, en respuesta a solicitudes de acceso a la información realizadas por R3D, dichas fiscalías reportaron haber realizado 37, 96, 116 y 586, respectivamente, siendo amplias las discrepancias detectadas.

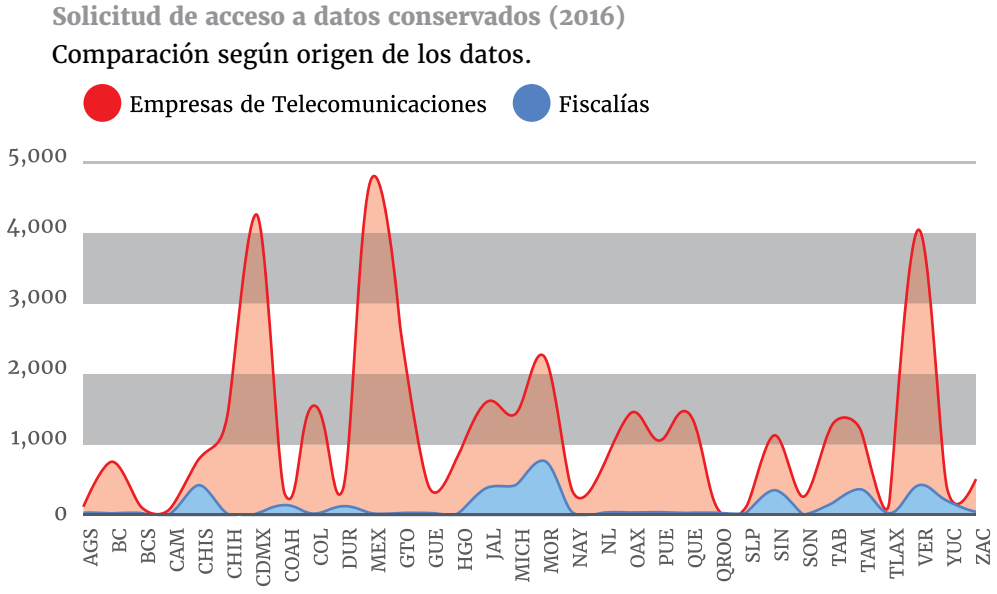
Se aprecian aún más inconsistencias si se contrasta la información estadística reportada en respuesta a solicitudes de acceso a la información con la publicada por las concesionarias en materia de telecomunicaciones respecto de los años 2016 y 2017.

Por ejemplo, en respuesta a solicitudes de acceso a la información, la entonces Procuraduría General de la República (PGR) reportó haber realizado 10,444 solicitudes de acceso a datos conservados en 2016 y 7,073 en 2017. Sin embargo, según los datos reportados por empresas de telecomunicaciones, la PGR solicitó la entrega de datos conservados en 13,052 ocasiones en 2016 y 12,160 veces en 2017, una discrepancia del 25% en 2016 y 72% en 2017.

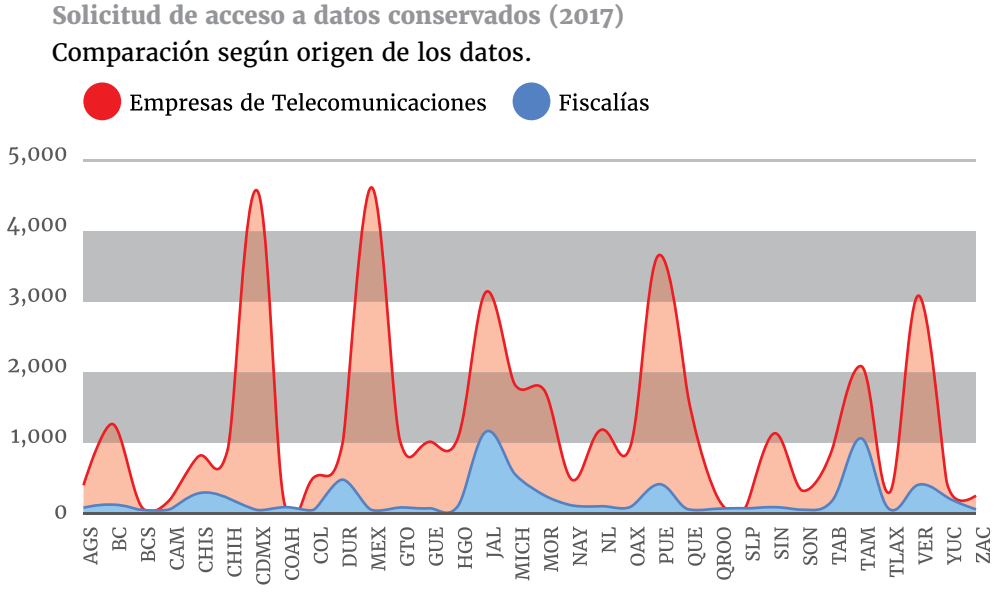
Las empresas de telecomunicaciones reportaron haber recibido solicitudes de acceso a datos conservados de otras autoridades federales como el CISEN, la Secretaría de Hacienda y Crédito Público (SHCP) y la Secretaría de Marina, a pesar de que estas reportaron cero (0) en respuesta a solicitudes de acceso a la información y de que algunas de dichas autoridades ni siquiera poseen facultades legales para llevar a cabo dichos requerimientos.

99. Guardia Nacional, Respuesta a la Solicitud de Información 2800100074421.

En el caso de las Fiscalías Estatales las discrepancias son también notorias y generalizadas, como se aprecia en las siguientes gráficas:



Gráfica 3.7. *Respuestas a solicitudes de acceso a la información y Reportes de empresas de telecomunicaciones.*



Gráfica 3.8. *Respuestas a solicitudes de acceso a la información y Reportes de empresas de telecomunicaciones.*

Adicionalmente, existen otros indicios de un mayor subregistro derivado del abuso del mecanismo excepcional contemplado en el artículo 303 del CNPP, para solicitar directamente el acceso a datos conservados a las empresas de telecomunicaciones sin control judicial previo y sujeto a la ratificación posterior por parte de la autoridad judicial federal.

Por un lado, a partir de los datos obtenidos mediante solicitudes de acceso a la información entre 2016 y 2019, las autoridades admiten que al menos el 57.3% de las solicitudes reportadas fueron realizadas sin control judicial previo, de las cuales el 76.7% fueron realizadas invocando las causales de excepción a las que se refiere el artículo 303 del CNPP y de ellas, el 39.5% no fueron ratificadas total o parcialmente.

Así mismo, existen indicios de que un número importante de solicitudes de acceso a datos conservados en las que se invoca el mecanismo excepcional no son sometidas a ratificación por parte de la autoridad judicial federal.[100]

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.[101]

La Fiscalía solicitó esta información a la empresa de telecomunicaciones Telcel, argumentando que estos datos serían utilizados en investigaciones sobre secuestros y desapariciones 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

100. Abi-Habib, Maria, et. al., "Políticos y funcionarios, blanco de vigilancia en México", *The New York Times*, 9 de noviembre de 2023, disponible en: https://www.nytimes.com/es/2023/11/09/espanol/mexico-vigilancia-fiscalia-telcel.html

101. *Ibidem*.

Doretti, y la defensora de derechos humanos Ana Lorena Delgadillo, quienes señalaron que la Subprocuraduría Especializada en Investigación de Delincuencia Organizada (SEIDO) accedió a sus registros telefónicos al incluirlas en en la misma carpeta donde se investigaba a integrantes de una organización delictiva.[102]

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 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.

2. Tecnologías de vigilancia detectadas en México

Con independencia de las medidas de vigilancia realizadas por diversas autoridades que cuentan con la colaboración de empresas de telecomunicaciones, en las últimas décadas se ha do-

102. R3D, "SEIDO accedió a registros telefónicos para espiar a periodista y defensoras por investigar masacre de San Fernando", 26 de noviembre de 2021, 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/

cumentado la utilización de diversas tecnologías de vigilancia desplegadas de manera directa por autoridades, frecuentemente sin control judicial, sin contar con facultades para llevar a cabo las mismas, con opacidad y de manera abusiva.

A continuación se detallan los distintos tipos de tecnologías detectadas, sus características y la evidencia de su utilización en México.

A. Spyware

Una de las tecnologías de vigilancia más poderosas que se ha detectado es el uso de sistemas de vigilancia conocidos como ***spyware***. En palabras de la Relatora Especial sobre la lucha contra el terrorismo (traducción propia del inglés al español; énfasis añadido):

> *[El spyware es un] software capaz de realizar intrusiones selectivas encubiertas y no detectadas e inspeccionar redes, ordenadores y dispositivos. Este tipo de software de intrusión* ***permite acceder a dispositivos fijos y móviles de modo que el contenido de las comunicaciones*** *de los usuarios y otra información, incluidos los metadatos (entre ellos, la ubicación, la duración, la fuente y el destinatario de dichas comunicaciones),* ***puedan controlarse de forma encubierta y remota****. Estas herramientas tecnológicas suelen conocerse como "spywares", y como tales se denominan en este documento, aunque, dada la naturaleza encubierta y las capacidades secretas de algunas de estas herramientas,* ***no es posible una definición exhaustiva de las características de la tecnología de los spyware****.*[103]

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.[104] Es decir, la tecnología empleada por un *spyware* da a sus usuarios no solo la habilidad de monitorear a la persona, sino también de manipular el dispositivo infectado, incluyendo la alteración, borrado o, incluso, implantación de información incriminante.

---

103. Relatora Especial sobre la Lucha contra el Terrorismo, *Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach*, abril 2023, pár. 15.

104. Resolución de la Asamblea General de las Naciones Unidas, "El derecho a la privacidad en la era digital", A/HRC/39/29, 3 de agosto de 2018, pár. 19, disponible en: https://www.ohchr.org/en/documents/thematic-reports/ahrc3929-right-privacy-digital-age-report-united-nations-high
19. 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.

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.[105]

En la actualidad, la gran mayoría de las herramientas de vigilancia utilizadas por los organismos estatales se obtienen del sector privado. Entre las empresas privadas responsables de este tipo de herramientas se encuentran las israelíes *NSO Group*,[106] *Quadream*[107] y *Candiru/Saito Tech*,[108] la británica *Gamma International Ltd*, las alemanas *Vilicius Holding GmbH* y *Trovicor GmbH*,[109] las francesas *Qosmos* y *Amesys*, las italianas *Area SpA*[110] y *Hacking Team/Memento Labs*,[111] la empresa *Cytrox*, con divisiones en Macedonia del Norte, Israel y Hungría,[112] las estadounidenses *Cyberpoint*, *Narus* (filial de *Boeing*), *BlueCoat Systems*[113] y *Cisco Systems*, y la emiratí *Darkmatter*,[114] entre otras.

---

105. Resolución de la Asamblea General de las Naciones Unidas, "El derecho a la privacidad en la era digital", A/HRC/51/17, 4 de agosto de 2022, pár. 8, disponible en: https://www.ohchr.org/en/documents/thematic-reports/ahrc5117-right-privacy-digital-age

106. AL OTH 211/2021 y AL/ISR 7/2021, aunque NSO también tiene operaciones en otros lados. *Véase:* AL BGR 2/2021.

107. *Véase*: Megiddo G., "Secretive Israeli cyber firm selling spy-tech to Saudi Arabia", *Haaretz*, 8 de junio de 2021, disponible en: https://www.haaretz.com/israel-news/tech-news/.premium.HIGHLIGHT-the-secret-israeli-cyber-firm-selling-spytech-to-saudia-arabia-1.9884403

108. *Véase*: Ziv A., "Top secret Israeli cyberattack firm revealed", *Haaretz*, 4 de junio de 2019, disponible en: https://www.haaretz.com/middle-east-news/.premium-top-secret-israeli-cyberattack-firm-revealed-1.6805950

109. Antes de su reestructuración, tras la insolvencia de diciembre de 2021, se llamaba FinFisher GmbH. *Véase*: Open Corporates, Vilicius Holding GmbH, disponible en: https://opencorporates.com/companies/de/D2601V_HRB205476

110. *Véase*: Ferrarella L., "Assad intercettava gli oppositori al regime con tecnologia made in Italy", *Corriere della Serra*, 1 de diciembre de 2016, disponible en: https://milano.corriere.it/notizie/cronaca/16_dicembre_01/assad-siria-intercettazioni-intercettava-oppositori-regime-tecnologia-made-italy-2420c69e-b7b1-11e6-a82f-f4dafb547583.shtml

111. Hacking Team fue adquirida en 2019 por Memento Labs. *Véase*: O'Neill P., "The fall and rise of a spyware empire", *MIT Technology Review*, 29 de noviembre de 2019, disponible en: https://www.technologyreview.com/2019/11/29/131803/the-fall-and-rise-of-a-spyware-empire/

112. *Véase:* Marczak, Bill, et al., "Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware", *The Citizen Lab*, 16 de diciembre de 2021, disponible en: https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

113. *Véase*: Parlamento Europeo, Departamento Temático de Derechos de los Ciudadanos y Asuntos Constitucionales, "Pegasus and surveillance spyware", mayo 2022, disponible en: https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf

114. *Véase*: Mazzetti M. & A. Goldman, "Ex-US intelligence officers admit to hacking crimes in work for Emiratis", *The New York Times*, 14 de septiembre de 2021, disponible en: https://www.nytimes.com/2021/09/14/us/politics/dark-matter-uae-hacks.html

La infección de dispositivos con software de vigilancia ocurre usualmente como consecuencia de la explotación de vulnerabilidades en redes, sistemas y dispositivos que suelen no ser conocidas por las proveedoras o fabricantes (*zero day exploits*), poniendo en riesgo la privacidad y seguridad de todas las usuarias de esos servicios. Esta forma de vigilancia no solamente es cuestionable éticamente, sino que, al no estar regulada la utilización de este método de vigilancia de manera específica en alguna ley en México, también es cuestionable desde el punto de vista legal.

En este sentido, el Alto Comisionado de las Naciones Unidas para los Derechos Humanos ha señalado que existen pruebas preocupantes de que diversos Estados pueden estar desplegando tecnología de vigilancia para identificar y rastrear a personas que posteriormente son objeto de detenciones arbitrarias, violencia ilegal, tratos inhumanos e incluso ejecuciones extrajudiciales. De igual forma, el anterior Relator Especial de la ONU sobre la promoción y protección del derecho a la libertad de opinión y de expresión, David Kaye, ha establecido que las intrusiones con *spyware* son muy difíciles de limitar en atención a las siguientes consideraciones (traducción propia del inglés al español; énfasis añadido):

> *Las herramientas de vigilancia analógicas, como la intervención de un teléfono fijo o móvil, suelen permitir el acceso a las conversaciones – lo que en sí constituye un problema potencial, pero no el vasto acceso a los contactos, los datos de localización, las pulsaciones de teclas, los vídeos, etc. de una persona. Es contenible en su objetivo tanto por orden judicial como tecnológicamente.* ***Spywares como Pegasus, por el contrario, pueden no ser tan limitantes. Su intrusión es difícil de limitar. En términos jurídicos, puede ser difícil, sino imposible, que un Estado demuestre que utiliza el spyware con fines limitados y sin "colateralmente" abordar datos personales que no tienen relevancia con un propósito gubernamental legítimo.***[115]

Por lo tanto, la Relatora Especial sobre la lucha contra el terrorismo ha establecido que para que dicha tecnología esté en línea con los derechos humanos debe existir (traducción propia del inglés al español; énfasis añadido):

> *[...] un análisis desde el punto de vista de los derechos humanos del uso de spywares en el contexto de la lucha antiterrorista sugiere que la tecnología de spywares* ***debe, como mínimo (a) permitir que los usuarios seleccionen específicamente determinados datos y metadatos,*** *en lugar de vigilar y registrar automáticamente todos los datos y metadatos;* ***b) evitar el acceso automático a los datos relativos a los contactos de las personas seleccionadas,*** *a menos que los usuarios requieran específicamente esa información adicional con fines de investigación;* ***c) diseñar mecanismos para impedir un uso perjudicial, como sistemas de señalización e "interruptores de desactivación" en casos de aparente uso indebido****; y, en cualquier caso,* ***(d) crear un registro auditable indeleble, permanente e ineditable de las acciones realizadas por el usuario del spyware,*** *incluidas las interferencias/mo-*

115. Kaye, D., "The Spyware State and the Prospects for Accountability", *Global Governance*, 2021, 27(4), 483-492, p. 492.

dificaciones de datos/metadatos, cuándo se produjeron y por quién fueron efectuadas, de modo que pueda verificarse el uso de la herramienta y las autoridades judiciales puedan evaluar a posteriori su respeto de los derechos humanos.[116]

Por todas las razones anteriores, la comunidad internacional crecientemente ha reconocido la importancia de restringir el uso de tecnologías de *spyware*.[117] Tanto el Alto Comisionado de la ONU para los Derechos Humanos, varios relatores especiales de la ONU, los líderes de las principales organizaciones de derechos humanos y distintos países se han unido a una petición de moratoria.[118] El Departamento de Comercio de Estados Unidos incluyó a *NSO Group* y a otras empresas israelíes de software espía en su lista de entidades restringidas, prohibiendo al gobierno estadounidense hacer negocios con ellas.[119] *Apple*[120] y *Meta*[121] han demandado a *NSO Group* por utilizar su infraestructura para vigilar teléfonos de personas.

En México, la adquisición y abuso de tecnologías de *spyware* han sido ampliamente documentadas. A continuación se sintetizan los principales hallazgos.

---

116. Relatora Especial sobre la Lucha contra el Terrorismo, *Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach, op. cit.*, pár. 126, p. 85.
On the contrary, as set out above, a human rights analysis of the use of spyware in the counter-terrorism context suggests that spyware technology must at a minimum: (a) allow for users to specifically target certain data and metadata, rather than automatically monitor and record all data and metadata; (b) avoid automatically accessing data relating to contacts of targeted individuals, unless users specifically require that additional information for investigative purposes; (c) engineer mechanisms to prevent harmful use, such as flagging systems and 'kill switches' in cases of apparent misuse;264 and, in any event, (d) create an indelible, permanent, and uneditable auditable record of what actions have been taken by the user of the spyware, including any interferences/modifications of data/ metadata, when those occurred, and by whom they were effected so that the use of the tool can be verified, and its human rights compliance assessed after the fact by judicial authorities.

117. The White House, "Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware", 18 de marzo de 2024, disponible en: https://www.whitehouse.gov/briefing-room/statements-releases/2024/03/18/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/

118. Oficina del Alto Comisionado de la ONU para los Derechos Humanos, "La CIDH, su RELE y ONU-DH México manifiestan preocupación ante nuevos hallazgos sobre la utilización del software Pegasus", 31 de enero de 2022, disponible en: https://hchr.org.mx/comunicados/la-cidh-su-rele-y-onu-dh-mexico-manifiestan-preocupacion-ante-nuevos-hallazgos-sobre-la-utilizacion-del-software-pegasus/; Hendin, Rebeca, "Más de 100.000 personas reclaman a los Estados de la ONU que pongan fin a la crisis de los programas espía", *Amnistía Internacional*, 28 de octubre de 2022, disponible en: https://www.amnesty.org/es/latest/news/2022/10/100000-people-urge-un-states-to-end-spyware-crisis/; "Alto a Pegasus: Costa Rica es el primer país en pedir una moratoria a los softwares de espionaje", *Access Now*, 13 de abril de 2022 [actualizado el 26 de enero de 2023], disponible en: https://www.accessnow.org/press-release/costa-rica-primer-pais-moratoria-spyware/

119. U.S. Department of Commerce, "Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities", 3 de noviembre de 2021, disponible en: https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list

120. "Apple demanda a NSO Group para contener el abuso de programas espía con patrocinio estatal", 23 de noviembre de 2021, Comunicado de Prensa Apple, disponible en: https://www.apple.com/co/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/

121. "Court orders maker of Pegasus spyware to hand over code to WhatsApp", *The Guardian*, 29 de febrero de 2024, disponible en: https://www.theguardian.com/technology/2024/feb/29/pegasus-surveillance-code-whatsapp-meta-lawsuit-nso-group

a. FinFisher de Gamma International

Según la información de su sitio web oficial, ***FinFisher***, entre otras herramientas y servicios, ofrece una *"solución estratégica de interceptación y vigilancia a gran escala"*. Aunque existe una versión de escritorio del programa para *Windows*, *MacOS* y *Linux*, el mayor peligro proviene de las infecciones en dispositivos móviles tanto de *iOS* como *Android*.

En 2014, el hacker Phineas Phisher logró vulnerar la seguridad de la compañía ***Gamma International UK Ltd*** ("Gamma"), productora de *FinFisher* (también conocido como *FinSpy*), y liberó las especificaciones de sus herramientas. De acuerdo con una investigación de la empresa de seguridad informática *Kaspersky*,[122] para infectar a los dispositivos en *iOS*, los vectores a través de SMS, correo electrónico y *WAP push* solo funcionaban si el dispositivo fue modificado para eliminar limitaciones impuestas por el fabricante del sistema operativo (*jailbreak*). Por lo que, si no ha pasado por este proceso, la única forma de infección requería el acceso físico.

En cambio, para infectar un dispositivo *Android*, *FinSpy* buscaba aprovecharse de herramientas como *SuperSU* y *Magisk*, así como utilizar una vulnerabilidad de seguridad (*exploit*) conocido como *DirtyCow* para tener privilegios de superusuario o administrador (*root*).

Este software permitía recopilar información personal como contactos, mensajes SMS/MMS, correos electrónicos, calendarios, ubicación GPS, fotos, archivos en la memoria, grabaciones de llamadas telefónicas e interceptar mensajes instantáneos. Tiene la capacidad de espiar muchos servicios de comunicación: *WhatsApp*, *WeChat*, *Viber*, *Skype*, *Line*, *Telegram*, así como *Signal* y *Threema*. Además de mensajes, *FinSpy* extrae archivos enviados y recibidos por las víctimas en aplicaciones de mensajería, así como datos sobre grupos y contactos.

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.[123] El entonces Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) anunció el inicio de una investigación,[124] sin embargo no se informó ningún resultado relevante.

---

122. Shoshin, Pavel, "FinSpy — commercial spyware", *Kaspersky Daily*, 10 de julio de 2019, disponible en: https://www.kaspersky.com/blog/finspy-commercial-spyware/27606/

123. Marczak, Bill, *et. al.*, "Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation", *The Citizen Lab*, 15 de octubre de 2015, disponible en: https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

124. Instituto Federal de Acceso a la Información y Protección de Datos, "El IFAI atiende desde el 20 de junio de 2013 denuncia sobre presuntas irregularidades por uso de programa Finfisher", Comunicado IFAI/064/13, 5 de julio de 2013, disponible en: https://inicio.inai.org.mx/Comunicados/Comunicado%20IFAI-064-13.pdf

En 2018, la empresa desarrolladora actualizó y mejoró el *spyware* cifrando algunas de sus funciones con el objetivo de infectar teléfonos inteligentes con *Android* e *iOS*. De acuerdo con *Kaspersky*, una de las principales características de estas nuevas versiones del *malware* es que sus desarrolladores han rehecho parte de su código, añadiendo cifrado para ocultar su rastro, haciendo más difícil su detección y más complejo su análisis.

Kaspersky ha documentado ataques de estas nuevas versiones en al menos 20 países, incluyendo una docena de infecciones en Myanmar. Aunque no se sabe cuántos ataques ha habido en el mundo, los investigadores sospechan que pueden ser muchos más de los conocidos, debido a la amplia cartera de clientes que ha tenido *Gamma*, incluyendo países como México, Uganda y Etiopía.

La organización no gubernamental *Privacy International* presentó una queja ante el Punto Nacional de Contacto para la Conducta Empresarial Responsable ("PNC") de Reino Unido[125] contra la firma *Gamma*. En la misma, alegaba que la empresa había exportado tecnología de vigilancia intrusiva en forma de herramientas de inspección profunda de paquetes (DPI, *deep packet inspection*) y *spywares* a las autoridades de Baréin, que fueron utilizados para vigilancia ilegal que condujo a violaciones de los derechos a la privacidad y a la libertad de expresión de los activistas de derechos humanos Ala'a Shehabi, Husain Abdulla y Shehab Hashem, así como a la detención arbitraria y tortura del activista Abdul Ghani Al-Khanjar.[126]

Gamma se negó a confirmar si había provisto o no del *spyware* a Baréin y, en consecuencia, el PNC no verificó ningún vínculo directo entre la empresa y los impactos adversos sobre los derechos humanos de la vigilancia digital en dicho país, pero sí concluyó que no había llevado a cabo la debida diligencia, asumido una política comprometida con el respeto a los derechos humanos ni provisto, o cooperado con, la reparación en los impactos sobre los derechos humanos. En consecuencia, el PNC concluyó que el enfoque de *Gamma* no era consistente con las obligaciones generales de respetar los derechos humanos y que "*el compromiso general de la empresa con el proceso ante el PNC había sido insatisfactorio, en particular en vista de la gravedad de las cuestiones planteadas*".[127]

---

125. En virtud de las Directrices de la OCDE — que han sido adoptadas por 38 gobiernos miembros de la OCDE y 12 no adheridos—, los gobiernos están obligados a establecer mecanismos no judiciales de reclamación, conocidos como PNC, cuya función es recibir quejas sobre el presunto incumplimiento por parte de las empresas de sus responsabilidades en materia de derechos humanos. A pesar de que el sistema sólo se aplica a las empresas registradas en el grupo de países participantes, una mayoría sustancial de las empresas de tecnología de vigilancia entran dentro de ese ámbito.

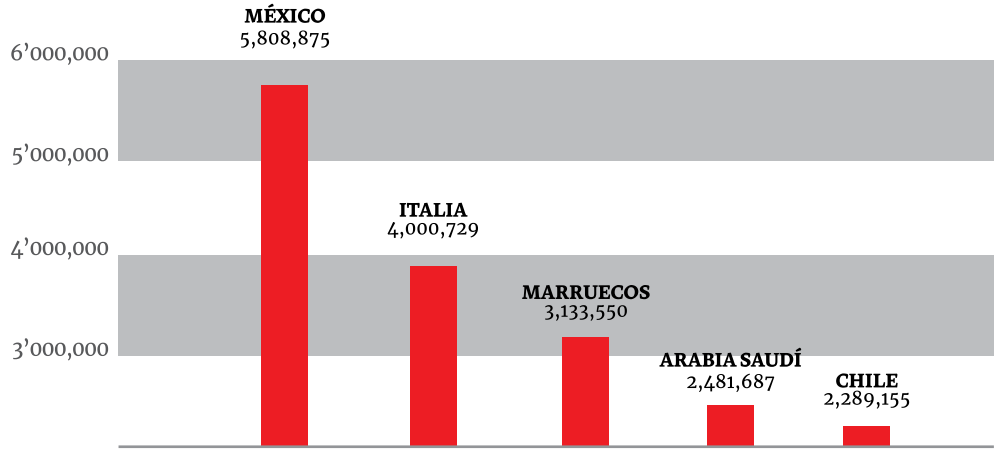
126. *Véase*: UK NCP, 'Privacy International & Gamma International UK Ltd: Final Statement After Examination of Complaint', diciembre 2014, ('UK NCP Final Statement'), disponible en: https://assets.publishing.service.gov.uk/media/5dd4154440f0b606eab6423c/UK-NCP-Final-statement-complaint-Privacy-International-Gamma-International-UK-Ltd.pdf

127. Traducción propia al español. UK NCP Final Statement, [70].

A pesar de esa conclusión adversa, no hay evidencia de que *Gamma* haya modificado alguno de sus procesos a fin de prevenir o mitigar impactos adversos sobre los derechos humanos en el futuro. En 2015, el PNC del Reino Unido solicitó una actualización respecto de tales avances, pero *Gamma* no respondió, lo que llevó al PNC a observar que "*solo puede concluir que [Gamma] no ha hecho ningún progreso (o esfuerzo) hacia el cumplimiento de las recomendaciones formuladas*" por el PNC[128], y que "*la falta de compromiso de Gamma es [...] una elección individual más que un resultado inevitable de la naturaleza de su negocio. Se trata de una elección que probablemente deje a Gamma expuesta a nuevos reclamos y desafíos, así como a suposiciones negativas por parte de las partes interesadas*".[129]

b. Galileo de Hacking Team

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.[130] En estos, 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 Baréin, 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[131] 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*.



Gráfica 3.9. *Gasto en Hacking Team por países (en euros). Correos filtrados de Hacking Team.*

128. Traducción propia al español. UK NCP Follow Up Statement, [9].

129. Traducción propia al español. UK NCP Follow Up Statement, [11].

130. Privacy International, "Surveillance company Hacking Team exposed", 6 de julio de 2015, disponible en: https://www.privacyinternational.org/press-release/1031/surveillance-company-hacking-team-exposed

131. Angel, A., "México, el principal cliente de una empresa que vende software para espiar" *Animal Político*, 7 de julio de 2015, disponible en: http://www.animalpolitico.com/2015/07/empresa-de-hackers-exhibida-por-venta-de-software-espia-a-paises-represores-y-mexico-resulta-su-principal-cliente/

Los correos también revelan que múltiples instituciones federales y de las entidades federativas negociaron, adquirieron y/o utilizaron los productos de *Hacking Team*. La investigación publicada en este informe ha sido posible gracias a la lectura y análisis de cientos de correos electrónicos disponibles en el repositorio ***Hacking Team Archive***,[132] publicado por *Wikileaks*.[133]

Entre los gobiernos locales mencionados con relaciones comerciales con *Hacking Team* se encuentran: Baja California, Campeche, Chihuahua, Durango, Estado de México, Guerrero, Jalisco, Nayarit, Puebla, Querétaro, Tamaulipas y Yucatán; así como dependencias como la Secretaría de la Defensa Nacional (Sedena), el Centro de Investigación y Seguridad Nacional (CISEN), la Policía Federal, la Procuraduría General de la República (PGR) y Petróleos Mexicanos (Pemex).

i. Una radiografía a Galileo

Una de las revelaciones de los correos filtrados de Hacking Team es el sistema de control remoto ***Galileo (Remote Control System)***, una plataforma que permite gestionar operaciones de vigilancia. El RCS funciona a través de un Agente que se instala en un dispositivo del Objetivo. Una vez ahí, el Agente transmite la información hacia una cadena de Anonimizadores, que se encarga de hacerla llegar al Recolector. Una vez que los datos ingresan a un "*ambiente seguro*", son manipulados y monitoreados en el Nodo Maestro. Los usuarios del sistema pueden conectarse al Nodo Maestro a través de una consola RCS para revisar la información.[134]

132. Disponible en: https://wikileaks.org/hackingteam/emails/

133. Velazco, C., "Now you can explore Hacking Team's world of selling spyware" Engadget, 10 de julio de 2015, disponible en: https://www.engadget.com/2015/07/10/hacking-team-email-archive/

134. La explicación sobre el funcionamiento del sistema, junto con la tabla de componentes, provienen de Hacking Team (2015) RCS 9.6. *The hacking suite for governmental interception. System administrator manual*. Disponible en: https://wikileaks.org/hackingteam/emails/fileid/1062729/494383

El siguiente gráfico ilustra la arquitectura del sistema:

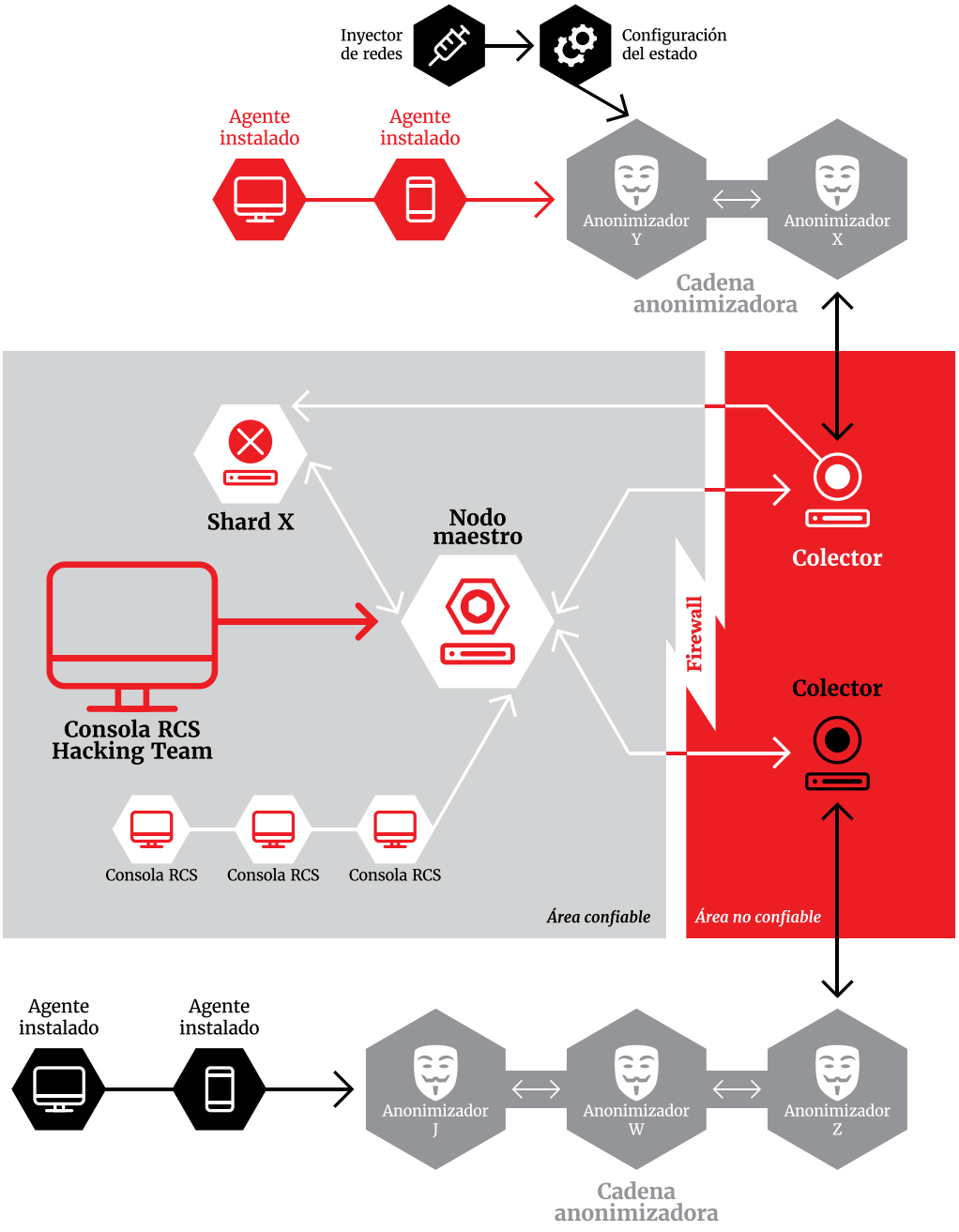


Gráfico 3.1. *Funcionamiento del software Galileo (RCS). Correos filtrados de Hacking Team.*

La siguiente tabla explica cada componente del sistema:

	Componente	Función
	**Agente** *(Agent)*	Software que irrumpe en el dispositivo, graba y comunica la información y datos del objetivo (*target*) hacia un anonimizador (*Anonymizer*).
	**Anonimizador** *(Anonymizer)*	Los anonimizadores están distribuidos geográficamente para garantizar el anonimato del Recolector, redirigiendo los datos recabados por el Agente o por los Inyector de Redes para proteger a los servidores de ataques remotos. Varios anonimizadores pueden ser colocados en una cadena para incrementar el nivel de protección. Se instalan en servidores privados virtuales (VPS).
	**Recolectores** *(Recollector)*	Cada cadena de anonimizadores cuenta con un recolector, que se divide en tres funciones: 1) recabar los datos e información enviados al último anonimizador, 2) mandar esta información a una partición horizontal (*shard*) o al nodo maestro (*Master Node*), y 3) recibe el estado actual del anonimizador y le envía actualizaciones o nuevas configuraciones.
	**Cortafuegos** *(Firewall)*	El *firewall* es opcional, pero altamente recomendable, ya que protege al entorno "confiable" (donde los datos se guardan y se procesan), del entorno "no confiable" (donde los datos son recabados).
	**Consola RCS** *(RCS Console)*	La consola de configuración, monitoreo y análisis es operada por los trabajadores del centro de vigilancia.
	**Nodo Maestro** *(Master Node)*	Es el corazón del servidor RCS, ya que maneja los flujos de datos, el estado de los componentes e incluye la primera partición horizontal de la base de datos. Incluye el servicio de Trabajador (*Worker*), que se encarga de desencriptar los datos antes de guardarlos en la base de datos, y el servicio de Monitor, que supervisa todos los componentes de la arquitectura y envía un correo electrónico en caso de alarma.

Tabla 3.3.a. *Componentes de la arquitectura de Galileo (RCS). Correos filtrados de Hacking Team.*

	Componente	Función
	**Inyector de Redes** *(Network Injector)*	El inyector de redes en un componente de hardware opcional, que puede ser fijo (*appliance*) o portátil (*tactical*). Se encarga de hacer operaciones para husmear (*sniffing*) o inyectar código en las conexiones HTTP del objetivo. Se comunica con el Recolector a través del Anonimizador para enviar datos y recibir instrucciones. Puede instalarse en proveedores de servicios de Internet (ISP), redes LAN alámbricas o inalámbricas (como oficinas u hoteles).
	**Partición horizontal** *(Shard)*	La partición horizontal es un diseño de base de datos que permite separar la base en hileras, en lugar de columnas; cada partición puede colocarse en un servidor separado. Esto permite distribuir la base de datos en varias máquinas. Cada partición incluye el servicio de Trabajador (*Worker*).
	**Objetivo** *(Target)*	El objetivo se refiere a la persona que está siendo vigilada. Cada dispositivo que posee es una fuente de datos y puede ser monitoreado por un agente.

Tabla 3.3.b. *Componentes de la arquitectura de Galileo (RCS). Correos filtrados de Hacking Team.*

La arquitectura del RCS también permite dos modelos de comunicación con otros sistemas RCS:

» **Uno a varios:** un sistema RCS recibe toda la evidencia de los agentes y la distribuye a otros sistemas RCS para mostrar y procesar solo la información que sea de su interés.

» **Varios a uno:** varios sistemas RCS reciben información de los agentes y envían todos los datos a un sistema RCS central que muestra y procesa todo.

ii. Métodos de infección y su uso en México

Para que el agente pueda instalarse dentro del dispositivo del objetivo, es necesario que exista un vector de infección; es decir, una puerta de entrada del *malware* al dispositivo objetivo (como un teléfono móvil). Entre los mecanismos que han sido aplicados en México, se encuentran el uso de archivos *exploit*, los inyectores de redes (aplicación y táctico), y los mensajes *WAP push*. Existen registros de estos cuatro métodos utilizados en el país entre 2013 y 2015.

Archivo *exploit*: *Hacking Team* define a un *exploit* como "*un código que, al explotar una falla o una vulnerabilidad, ejecuta un código imprevisto. Es usado para infectar dispositivos del objetivo*". De acuerdo con los correos filtrados, los usuarios finales solicitaron, a través de *tickets* (turnos) del sitio de soporte de *Hacking Team*, la creación de estos archivos para infectar a los objetivos. Al hacer clic en el fichero, se hace la carga del agente y el dispositivo queda comprometido.

Una característica importante es el uso de ingeniería social[135] para aumentar la efectividad de las infecciones por esta vía. Los casos de Puebla y Querétaro son ilustrativos en este sentido. En Puebla, el gobierno del Estado utilizó el nombre de actores políticos para incentivar los clics.[136] De forma similar, el gobierno de Querétaro empleó documentos como resoluciones de solicitudes de información para dirigirse a periodistas y sociedad civil.[137] Otro ejemplo es la Secretaría de la Defensa Nacional, que preguntó en una demostración "*cómo saber qué exploit pedirle a HT [Hacking Team]*" o si "*podían entrenarlos en ingeniería social*".[138]

Además de los casos mencionados, se detectó el uso de *exploits* por parte de entidades como Baja California[139], Yucatán,[140] Jalisco[141] y el CISEN, que incluso solicitó ayuda para que "*los exploits pudieran funcionar dos o tres veces antes de ser borrados.*"[142]

Inyector de redes táctico: El inyector de redes táctico (TNI) es una computadora portátil usada para instalación de agentes en redes LAN o WiFi. El TNI identifica los dispositivos en una red alámbrica o inalámbrica e inyecta los agentes. Se basa en la identificación manual o automática; o en reglas de inyección predeterminadas por la consola RCS. El TNI también puede conectarse a redes WiFi protegidas,

135. La ingeniería social es "la práctica de obtener información confidencial a través de la manipulación de usuarios". Colaboradores de Wikipedia (2016) Ingeniería social (seguridad informática), disponible en: https://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_inform%C3%A1tica)

136. Aroche Aguilar, E., "RMV infectó equipos con archivos exploit para espiar a opositores políticos", Lado B, 12 de julio de 2015, disponible en: http://ladobe.com.mx/2015/07/rmv-infecto-equipos-con-archivos-exploit-para-espiar-a-opositores-politicos

137. support@hackingteam.com (17 de enero de 2014) [!EUM-730-45911]: 12 exploits to 12 different persons. E-mail. Disponible en: https://www.wikileaks.org/hackingteam/emails/emailid/73139

138. Martínez, D. (6 de mayo de 2015) Report SEDENA Mexico. E-mail. Disponible en: https://wikileaks.org/hacking-team/emails/emailid/6431

139. Rodriguez-Solís y Guerrero, S. (10 de octubre de 2014) SEPYF project little summary. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/5761

140. Martínez, D. (12 de febrero de 2015) Re: Android Exploits fail on YUKI. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/916462

141. Vardaro, C. (22 de enero de 2015) Re: Exploit for training in JASMINE. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/632106

142. Milan, D. (20 de enero de 2014) Re: México Jan 2014. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/71965

simular un punto de acceso a una red WiFi, o desbloquear la contraseña del sistema operativo.

De acuerdo con la hoja de datos del TNI,[143] el ataque se efectúa de la siguiente manera:

> El Inyector de Redes Táctico es capaz de romper la seguridad de una red inalámbrica cuando la contraseña es desconocida, incluida la protección WEP, WPA y WPA2; incluye un diccionario de más de 45 millones de palabras para ataques basados en diccionario.
>
> El TNI apoya a la identificación del equipo a infectar mostrando varias informaciones sobre todos los individuos conectados a una red bajo ataque, incluyendo –pero no limitado a– la dirección IP, el nombre del equipo (*hostname*) y sitios web visitados.
>
> Todos los dispositivos identificados como objetivos pueden ser sujetos de distintos ataques, de acuerdo con reglas predeterminadas. Los vectores de infección incluyen la inyección de código en sitios web visitados y la fusión "al vuelo" del agente RCS con archivos ejecutables descargados por el objetivo.

Otras dos formas de infección mencionadas en la hoja de datos del TNI son: 1) la infección del objetivo mientras ve vídeo de *YouTube*, ya que el TNI fuerza una actualización de *Adobe Flash* que, una vez aceptada, instala el agente RCS en el dispositivo; y, 2) al reemplazar cualquier archivo en la web con otro archivo; por ejemplo, al suplantar un *.doc* descargado por el usuario objetivo con un *.doc* previamente fabricado para explotar una vulnerabilidad de día cero.

Entre los estados en México que adquirieron o mostraron interés en adquirir un TNI, se encuentran Campeche,[144] Chihuahua,[145] Guerrero,[146] Nayarit,[147] Puebla,[148] Tamaulipas[149] y Yucatán,[150] mien-

143. Hacking Team. Tactical Injector Network. Datasheet. https://wikileaks.org/hackingteam/emails/fileid/511703/237789

144. Scarafile, A. (17 de mayo de 2013) TNI in Stock. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/597097

145. Velasco, A. (17 de octubre de 2013) Re: HT at ISS Washington 2013. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/4560

146. Velasco, A. (24 de enero de 2014) Re: PGJ Guerrero in Milan. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/6566

147. Martínez, D. (20 de marzo de 2015) Report Demo Cyber Police Nayarit Mexico. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/5430

148. Mokotov, G. (11 de agosto de 2014) RE: COTIZACION HT PUEBLA. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/252042

149. Bettini, M. (30 de abril de 2014) Re: Prices for Neolinz. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/234499

150. Scarafile, A. (28 de octubre de 2014) Delivery Mexico (YUKI). E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/16339

tras que en dependencias federales se encuentran la Secretaría de la Defensa Nacional (Sedena),[151] el Centro de Investigación y Seguridad Nacional (CISEN)[152] y Petróleos Mexicanos (Pemex).[153]

> **Aplicación de inyector de redes:** La aplicación de inyector de redes (NIA) permite que el agente RCS sea inyectado en páginas web visitadas o archivos descargables a través del monitoreo de las conexiones del objetivo. La NIA analiza el tráfico de web del objetivo y, cuando ciertas condiciones se cumplen, inyecta el agente. Sus vectores de infección son muy similares al del TNI.

De acuerdo con *Hacking Team*, la NIA está diseñada para operar dentro de la red de un proveedor de servicios de Internet (ISP), monitoreando a los suscriptores y "*en caso de que la conexión de Internet del objetivo esté en un edificio con un red manejada de forma interna (por ejemplo, oficinas, hoteles, aeropuertos), la NIA también puede ser instalada dentro de ese edificio.*"

Entre los actores en México identificados con el uso de esta tecnología se encuentran Chihuahua[154] o Guerrero.[155]

> **Instalación Remota Móvil o *WAP-push*:** La Instalación Remota Móvil (RMI) es un mecanismo de infección que funciona mediante el envío de un mensaje *WAP-push* al *smartphone* objetivo. Cuando el SMS es recibido y aceptado por el usuario, el navegador automáticamente se abre y el paquete de instalación del agente es descargado de la URL incluida en el mensaje. El mensaje de texto puede ser personalizado, permitiendo el uso de técnicas de ingeniería social con amplitud: por ejemplo, al pretender ser el operador de telecomunicaciones ofreciendo promociones o actualizaciones, se incrementan dramáticamente las posibilidades de éxito para la instalación del agente.[156]

Al abrirse automáticamente el enlace en el navegador, el objetivo no necesita hacer clic para que se descargue el agente en su dispositivo, lo que representa un riesgo elevado. En México se

---

151. Martínez, D. (6 de mayo de 2015) Report SEDENA Mexico. E-mail. Disponible en: https://wikileaks.org/hacking-team/emails/emailid/6431

152. Rodriguez-Solís y Guerrero, S. (20 de febrero de 2014) SEGOB Day 1. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/237286

153. Velasco, A. (19 de diciembre de 2013) Pemex Contract. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/4459

154. Bettini, M. (26 de marzo de 2014) Re: RFQ. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/238221

155. Milan, D. (20 de enero de 2014) Re: México Jan 2014. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/71965

156. NICE Systems (2012) Section 2. RCS Hacking System. Disponible en: https://wikileaks.org/hackingteam/emails/fileid/445596/211695

ha documentado el uso de este método de infección en estados como Querétaro,[157] Guerrero,[158] Jalisco[159] y Puebla,[160] así como la SEDENA, que incluso preguntó a los técnicos de *Hacking Team* si había forma de modificar la cabeza de un mensaje.[161]

iii. Casos de venta y uso de Hacking Team en México

Los correos filtrados revelan detalles de las negociaciones, adquisiciones y casos de uso del *Remote Control System* de *Hacking Team* en México. En casi todos los casos, las operaciones fueron conducidas a través de empresas intermediarias, quienes ofrecieron el equipo de vigilancia a gobiernos estatales y dependencias federales. La siguiente tabla resume los clientes estatales potenciales y reales de la firma italiana en el país.

Cliente	Intermediarios	Negociación	Compra	Identificador
Gobierno de Baja California	Elite Tactical (Elite by Carga, subsidiaria de Grupo Armor)	Preventa en agosto de 2014	Entregado en septiembre de 2014	SEPYF / MVA
Gobierno de Campeche	Grupo Kabat / SYM Servicios Integrales		Entregado en mayo de 2013. Pago por 386 mil euros.	SDUC
Gobierno de Chiapas	Servicios Integrales Heres	Solicitud de reunión en junio de 2015	No se sabe	N/A
Gobierno de Chihuahua	Grupo RF (hasta marzo de 2014) Grupo Armor (desde agosto de 2014)	Reunión en Chihuahua en marzo de 2014. Carta del gobierno de Chihuahua en agosto de 2014	No se sabe. Cotización enviada en marzo de 2014	N/A
Gobierno de Durango	Elite Tactical (Elite by Carga, subsidiaria de Grupo Armor)	Hecha a la par de Baja California y Yucatán	Factura por 265 mil euros, en septiembre de 2014. Entregado en noviembre de 2014	DUSTIN

Tabla 3.4.a. *Clientes de Hacking Team de gobiernos estatales en México. Correos filtrados de Hacking Team.*

157. De Giovanni, F. (9 de mayo de 2013) food for thoughts. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/678813

158. Milan, D. (20 de enero de 2014) Re: México Jan 2014. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/71965

159. Scarafile, A. (11 de diciembre de 2014) Delivery Mexico (JASMINE). E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/5303

160. Catino, M. (3 de junio de 2013) Puebla Delivery (GEDP) - Report. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/590122

161. Martínez, D. (6 de mayo de 2015) Report SEDENA Mexico. E-mail. Disponible en: https://wikileaks.org/hacking-team/emails/emailid/6431

Cliente	Intermediarios	Negociación	Compra	Identificador
Ciudad de México (División de Narcóticos de la SSP)	CloudSec	Solicitud de contacto con HT en febrero de 2015	No se sabe	N/A
Procuraduría General de Justicia del Estado de México	DTXT Corp. (2012) Neolinx (desde noviembre de 2013)		Pago, entrega y capacitación en mayo-junio de 2012. Renovación en diciembre de 2013	PGJEM
Gobierno de Guerrero	Neolinx	Reuniones y demostraciones en enero de 2014	Contrato fechado a junio de 2014	N/A
Gobierno de Jalisco	Grupo Kabat / SYM Servicios Integrales		Entregado en diciembre de 2014. Facturas por 448 mil euros	JASMINE
Gobierno de Nayarit	CloudSec	Envío de propuesta de compra en mayo de 2015	No se sabe. Negada por el gobierno	N/A
Gobierno de Puebla	Grupo Kabat / SYM Servicios Integrales		Factura por 465 mil euros en abril de 2013. Instalado en junio de 2013	GEDP
Gobierno de Querétaro	TEVA/Binah-Lab		Compra e instalación en enero-febrero de 2013	EDQ
Gobierno de Sinaloa	Grupo Kabat / SYM Servicios Integrales (2013) Grupo Armor (desde marzo de 2014)	Precontrato entre Kabat y el gobierno en septiembre de 2013	No se sabe. Demostración en marzo de 2014	N/A
Gobierno de Sonora	Elite Tactical (Elite by Carga, subsidiaria de Grupo Armor) Neolinx (desde junio de 2015)	Reunión programada en diciembre de 2014	No se sabe. Solicitud de demostración en junio de 2015	N/A
Secretaría de Seguridad Pública de Tamaulipas	Grupo Kabat / SYM Servicios Integrales		Pago en junio de 2014. Entrega en julio de 2014	SSPT
Gobierno de Yucatán	Elite Tactical (Elite by Carga, subsidiaria de Grupo Armor) Axios Group, Proyecto Vlemer (prestanombres)		Entrega en noviembre de 2014	YUKI

Tabla 3.4.b. *Clientes de Hacking Team de gobiernos estatales en México. Correos filtrados de Hacking Team.*

De igual forma, existe evidencia de la adquisición del *spyware* desarrollado por *Hacking Team* por diversas autoridades federales como es el caso del CISEN, así como negociaciones con la Policía Federal, la Secretaría de la Defensa Nacional, la Secretaría de Marina, e incluso, con la empresa paraestatal Petróleos Mexicanos (PEMEX).

Se destaca que múltiples clientes de *Hacking Team* en México no poseen facultades legales para llevar a cabo la intervención de comunicaciones privadas, como es el caso de la Secretaría de Planeación y Finanzas de Baja California,[162] la Secretaría de Gobierno de Jalisco,[163] la Secretaría General de Gobierno de Puebla,[164] la Secretaría de Seguridad Pública de Tamaulipas y la paraestatal PEMEX.[165]

Además, existe evidencia de que la instalación del sistema *Galileo* desarrollado por *Hacking Team* ocurrió en oficinas de las empresas privadas que fungieron como intermediarias[166] e inclusive indicios de que el equipo utilizado para operar el sistema habría sido sustraído.

Por ejemplo, el 22 de junio de 2017, el gobernador de Guerrero Héctor Astudillo afirmó que el equipo de vigilancia adquirido por su predecesor se encontraba desaparecido. "*Lo que yo les quiero decir es que hemos buscado ese equipo, no lo encontramos, entonces no puedo yo asegurar que alguien lo compró, porque yo no lo encuentro*", afirmó el mandatario a *Proceso*.[167]

También existe evidencia del uso ilegal del sistema. Por ejemplo, en Puebla, el equipo fue instalado en el Centro de Análisis Prospectivo (CAP), una oficina de la Secretaría General del Gobierno de Puebla (SGG). De acuerdo a una investigación periodística, a inicios de 2013, el CAP fue convertido en un centro de espionaje a cargo de Eukid Castañón, entonces subsecretario de Asuntos Políticos y Protección Civil, y hombre cercano al gobernador Rafael Moreno Valle.

---

162. "Espía Gobierno a funcionarios y candidatos", *Zeta*, 14 de julio de 2015, disponible en: https://zetatijuana.com/2015/07/espia-gobierno-a-funcionarios-y-candidatos/

163. Sánchez Onofre, J., "Confirman espionaje electrónico de Jalisco", *El Economista*. 9 de julio de 2015, disponible en: https://www.eleconomista.com.mx/tecnologia/Confirman-espionaje-electronico-de-Jalisco-20150709-0159.html

164. Aroche Aguilar, E., "RMV infectó equipos con archivos exploit para espiar a opositores políticos", *Lado B*, 12 de julio de 2015, disponible en: http://ladobe.com.mx/2015/07/rmv-infecto-equipos-con-archivos-exploit-para-espiar-a-opositores-politicos

165. Busatto, F., "License for PEMEX and other hasp keys", 30 de julio de 2014, E-mail, disponible en: https://wikileaks.org/hackingteam/emails/emailid/245782

166. *Idem*.

167. Flores Contreras, E., "Astudillo afirma que el equipo de espionaje adquirido por su antecesor "desapareció"", *Proceso*, 22 de junio de 2017, disponible en: http://www.proceso.com.mx/492046/astudillo-afirma-equipo-espionaje-adquirido-antecesor-desaparecio

El equipo operó bajo las órdenes de Joaquín Arenal, un exdelegado del Centro de Investigación y Seguridad Nacional (CISEN); Héctor Arrona Hurrea, director del Centro de Análisis Prospectivo; y José Antonio Celorio Mansi, cuyo nombre fue revelado en los correos filtrados.[168] Los correos mostraron que el gobierno de Puebla solicitó, a través de la dirección electrónica soporteuiamx@gmail.com, una serie de *exploits* con fines de espionaje político, entre los meses de mayo de 2013 y junio de 2014.

Ninguna persona ha sido sancionada en México por las irregularidades en la adquisición y operación del *spyware*. Sin embargo, el empresario Carlos Guerrero admitió —ante una corte federal en los Estados Unidos en 2022— su culpabilidad por la venta de equipo de espionaje a diferentes gobiernos estatales en México y aceptó haber negociado con pleno conocimiento del uso ilegal de estos sistemas.[169]

Guerrero admitió haber vendido equipo de espionaje de la firma italiana *Hacking Team* a los gobiernos de Baja California y Durango a través de la empresa *Elite by Carga* entre 2014 y 2015. En su declaración, el empresario señaló que tenía conocimiento de que esos sistemas de vigilancia "*podían y probablemente serían utilizados con fines políticos*" e incluso confesó haber ayudado a un alcalde en Morelos a acceder ilegalmente a cuentas de correos y redes sociales de un oponente.

Guerrero también admitió que, entre 2016 y 2017, comercializó bloqueadores de señal, herramientas de intercepción de WiFi, antenas falsas de telefonía móvil (*IMSI catchers*) y la capacidad de *hackear* mensajes de *WhatsApp* de clientes prospectivos en Estados Unidos y México. Igualmente, Guerrero aceptó haber usado las tecnologías de vigilancia que vendía a gobiernos con fines comerciales y personales de clientes privados.

La admisión de Guerrero contradice la negativa que los gobiernos de Baja California, Durango y otras entidades federativas realizaron frente a la publicación de evidencia de adquisición de software espía de *Hacking Team*. Además, aporta aún más evidencia de que la compra y utilización de tecnologías de vigilancia en México se realizaron con fines distintos al combate a la delincuencia, como presumen las empresas que comercializan estos productos y los gobiernos que las adquieren.

---

168. Aroche Aguilar, E., "RMV infectó equipos con archivos exploit para espiar a opositores políticos", *Lado B*, 12 de julio de 2015, disponible en: http://ladobe.com.mx/2015/07/rmv-infecto-equipos-con-archivos-exploit-para-espiar-a-opositores-politicos

169. R3D, "Empresario se declara culpable de vender equipo de espionaje en México a sabiendas de su uso ilegal", 17 de febrero de 2022, disponible en: https://r3d.mx/2022/02/17/empresario-se-declara-culpable-de-vender-equipo-de-espionaje-en-mexico-a-sabiendas-de-su-uso-ilegal/

c. Pegasus de NSO Group

NSO Group Technologies es otra de las empresas cuyo nombre ha sido ampliamente vinculado a acciones de vigilancia en México.[170] La compañía israelí asegura dedicarse a "*proveer a gobiernos autorizados con tecnología que los ayude a combatir el terror y el crimen; la compañía vende solo a agencias gubernamentales autorizadas, y cumple cabalmente con estrictas leyes y regulaciones de control de exportaciones*".[171]

NSO Group Technologies afirma que su tecnología es utilizada exclusivamente por clientes gubernamentales aprobados por el Ministerio de Defensa de Israel.[172] 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 24 de agosto de 2016, el *Citizen Lab* de la Universidad de Toronto lanzó el informe *The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender*.[173] En dicho documento, los investigadores detallan el funcionamiento del *spyware* ***Pegasus***, el principal producto de *NSO Group*.

El método de infección original de *Pegasus* consistía en el envío de mensajes de texto que incluían enlaces con nombres de dominio que suplantaban la identidad de sitios de noticias (el más común),[174] del gobierno,[175] empresas de telecomunicaciones,[176] redes sociales,[177] aerolíneas.[178] También aplicaban *spear phishing*: ataques más personalizados que buscan que la persona acceda y comparta información de una de sus cuentas en línea (bancaria, personal, portal del trabajo, envíos en línea).[179]

---

170. Cox, J. & L. Franceschi Bicchierai, "Meet NSO Group, The New Big Player In The Government Spyware Business", *Motherboard*, 25 de agosto de 2016, disponible en: https://motherboard.vice.com/en_us/article/nso-group-new-big-player-in-government-spyware

171. Fox-Brewster, T., "Everything We Know About NSO Group: The Professional Spies Who Hacked iPhones With A Single Text", *Forbes*, 25 de agosto de 2016, disponible en: https://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/#366045ab3997

172. *Ibidem*.

173. Marczak, Bill & John Scott-Railton, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender," *Citizen Lab Research*, Reporte No. 78, University of Toronto, Agosto 2016, disponible en: https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

174. E.g.: unonoticias.net, univision.click y smsmensaje.mx. Esa fue la técnica usada para engañar al periodista Rafael Cabrera, que investigaba el caso de la "Casa Blanca" de Peña Nieto.

175. E.g.: mensajes a Aristegui, su hijo, y Loret de Mola sobre un problema con su visa de la embajada de EUA; mensajes de alerta AMBER.

176. E.g.: iusacell-movil. com.mx e ideas-telcel.com.mx

177. E.g.: youtube.com.mx, fb-accounts.com

178. E.g.: checkinonlinehere.com

179. E.g.: track-your-fedex-package.org

Sin embargo, desde hace varios años se ha detectado que el operador puede infectar un dispositivo con *Pegasus* sin necesidad de que el objetivo haga clic en ningún enlace ni descargue ningún archivo (infección sin clic).[180]

Pegasus proporciona a su operador acceso completo al dispositivo móvil de un objetivo, permitiéndole extraer contraseñas, archivos, fotos, historial web, contactos, así como datos de identidad (como información sobre el dispositivo móvil). También puede realizar capturas de pantalla y supervisar las entradas del usuario, así como activar el micrófono y la cámara del teléfono. Esto permite a los atacantes vigilar toda la actividad en el dispositivo y en las proximidades del mismo, como las conversaciones mantenidas en una habitación.[181]

Pegasus también permite al operador grabar los mensajes de chat que se envían y reciben, incluidos los mensajes enviados a través de aplicaciones de mensajería de texto cifradas o con mensajes que desaparecen, como *WhatsApp* o *Telegram*; así como las llamadas telefónicas y de *VoIP*, incluyendo las llamadas a través de aplicaciones de llamadas cifradas. Para algunos programas de chat, *Pegasus* también admite la extracción de registros de mensajes anteriores. De igual forma, permite al operador rastrear la ubicación del objetivo.

Igualmente, el *spyware* permite la modificación o manipulación de los datos de un dispositivo. Además, puede utilizarse para robar *tokens* que brinden acceso continuo a cuentas populares en la nube. Otra característica encontrada del *spyware* es que, una vez que infecta el dispositivo, deshabilita las actualizaciones automáticas del sistema operativo para garantizar su persistencia; también detecta y remueve otros *jailbreaks* en el aparato.

i. Primeros antecedentes de Pegasus en México

El primer antecedente de *Pegasus* en México se registró en 2012, cuando investigaciones periodísticas publicaron que la Secretaría de la Defensa Nacional (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 cuales ascendieron a 5.6 mil millones de pesos.[182] Dichas contrataciones sucedieron luego de una demostración

180. Marczak, Bill, *et. al.*, "NSO Group iMessage Zero-Click Exploit Captured in the Wild", *The Citizen Lab*, 13 de septiembre de 2021, disponible en: https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/

181. Marczak, Bill, *et. al.*, "NSO Group's Pegasus Spyware Returns in 2022 with a Trio of iOS 15 and iOS 16 Zero-Click Exploit Chains", *The Citizen Lab*, 18 de abril de 2023, disponible en: https://citizenlab.ca/2023/04/nso-groups-pegasus-spyware-returns-in-2022/

182. "Gobierno federal vía Sedena compró 5 mil mdp en equipo para espionaje", *Aristegui Noticias*, 16 de Julio de 2012, disponible en: https://aristeguinoticias.com/1607/mexico/gobierno-federal-via-sedena-compro-5-mil-mdp-en-equipo-para-espionaje/

del funcionamiento del sistema *Pegasus*, en mayo de 2011, al entonces presidente Felipe Calderón, así como al Secretario de Defensa Nacional, Guillermo Galván Galván.[183]

Un correo interno de la empresa *Hacking Team* (filtrado en 2015 por *Wikileaks*)[184] relata que la SEDENA adquirió *Pegasus* en 2011, pero que habían sido defraudados por Susumo Azano, director de *Security Tracking Devices*, quien les vendió también la construcción de un centro de monitoreo que terminó desierto.[185]

La Auditoría Superior de la Federación encontró irregularidades en cinco de los contratos suscritos por la SEDENA, por lo que solicitó al Órgano Interno de Control iniciar las averiguaciones correspondientes. No obstante, ocho meses después de abrir el expediente, el Ejército decidió archivar el caso por supuesta falta de elementos.[186]

En 2015, la Procuraduría General de la República (PGR) abrió una investigación por presunto lavado de dinero relacionado con dichas adquisiciones.[187] Sin embargo no se ha informado ninguna consecuencia derivada de la investigación.

La SEDENA admitió en 2022 que adquirió *Pegasus* del 27 de junio de 2011 al 24 de agosto de 2013. [188] No obstante, ha argumentado que "*fue empleado única y exclusivamente para mantener la seguridad y capacidad operativa del Ejército y Fuerza Aérea Mexicanos, mediante acciones de inteligencia*", las cuales afirma –falsamente– que se encuentra facultada a realizar conforme a la Ley Orgánica del Ejército y Fuerza Aérea Mexicanos y el artículo Quinto Transitorio de la Reforma Constitucional en materia de Guardia Nacional y Seguridad Pública. Ninguna de esas disposiciones le autoriza a llevar a cabo intervenciones de comunicaciones privadas.

En 2023, el diario *The New York Times* confirmó que el Ejército Mexicano se convirtió en el primer cliente internacional de *NSO Group* tras una negociación suscitada en un club de es-

183. R3D, "NSO Group mostró Pegasus a Felipe Calderón y su Secretario de Defensa", 11 de agosto de 2021, disponible en: https://r3d.mx/2021/08/11/nso-group-mostro-pegasus-a-felipe-calderon-y-su-secretario-de-defensa/

184. https://wikileaks.org/hackingteam/emails/emailid/8964

185. "Susumo Azano, el empresario que vendió a Sedena equipos de espionaje por 5 mil mdp", *Aristegui Noticias*, 21 de febrero de 2014, disponible en: https://aristeguinoticias.com/2102/mexico/susumo-azamo-el-empresario-que-vendio-a-sedena-equipos-de-espionaje-por-5-mil-mdd/

186. Gallegos, Z., "El Ejército mexicano archivó las indagatorias por la compra de Pegasus", *El País*, 3 de noviembre de 2021, disponible en: https://elpais.com/mexico/2021-11-04/el-ejercito-mexicano-archivo-las-indagatorias-por-la-compra-de-pegasus.html

187. "3 años después, PGR investiga estos contratos de equipo de espionaje de la Sedena", *Aristegui Noticias*, 14 de septiembre de 2015, disponible en: https://aristeguinoticias.com/1409/mexico/3-anos-despues-pgr-investiga-estos-contratos-de-equipo-de-espionaje-de-la-sedena/

188. Secretaría de la Defensa Nacional, "Comunicado de Prensa 161", 4 de octubre de 2022, disponible en: https://www.gob.mx/sedena/prensa/comunicado-de-prensa-161

triptís en marzo de 2011. Además, reveló que el Ejército no solo ha sido el cliente más antiguo de *Pegasus*, sino que también "*ha atacado a más teléfonos móviles con ese programa malicioso que cualquier otra agencia gubernamental del mundo*".[189]

ii. Gobierno Espía: ataques con Pegasus durante el gobierno de Enrique Peña Nieto (2014-2017)

En febrero de 2017, se hizo público que el Estado Mexicano utilizó el *spyware Pegasus* con propósitos de espionaje a defensores de derechos humanos cuya lucha se enfoca a combatir la obesidad a través del aumento de impuestos a las bebidas azucaradas, incluyendo al Director de la organización *El Poder del Consumidor*. Los ataques perpetrados contra los activistas tuvieron lugar mientras se planeaba una campaña en favor del impuesto a las bebidas azucaradas.[190]

En junio de 2017, *Citizen Lab*, en conjunto con *ARTICLE 19*, *Red en Defensa de los Derechos Digitales (R3D)* y *SocialTIC* publicamos el informe "*Gobierno Espía: Vigilancia sistemática a periodistas y defensores de derechos humanos en México*",[191] en el cual se da cuenta de múltiples casos de intentos de infección con el malware *Pegasus*.[192]

En el informe se documentan 76 mensajes de texto con enlaces que dirigen a dominios identificados como parte de la estructura de *NSO Group*. Esto implica que los mensajes analizados corresponden sin lugar a dudas a intentos de infección con el *malware Pegasus*.

Según investigaciones del *Citizen Lab*, los mensajes de texto utilizados para infectar dispositivos con el *spyware Pegasus* utilizaron dominios que suplantaban la identidad de sitios de noticias, empresas de telecomunicaciones y aplicaciones en Internet como:

---

189. Kitroeff, Natalie & Bergman, Ronnen, "How Mexico Became the Biggest User of the World's Most Notorious Spy Tool", *The New York Times*, 18 de abril de 2023, disponible en: https://www.nytimes.com/2023/04/18/world/americas/pegasus-spyware-mexico.html

190. Perlroth, Nicole, "Spyware's Odd Targets: Backers of Mexico's Soda Tax", *The New York Times*, 11 de febrero de 2017, disponible en: https://www.nytimes.com/2017/02/11/technology/hack-mexico-soda-tax-advocates.html?smid=fb-share&_r=0; Scott-Railton, John, *et. al.*, "Bitter Sweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links", *The Citizen Lab*, disponible en: https://citizenlab.org/2017/02/bittersweet-nso-mexico-spyware/; R3D, "Destapa la Vigilancia: promotores del impuesto al refresco, espiados con malware gubernamental", disponible en: https://r3d.mx/2017/02/11/destapa-la-vigilancia-promotores-del-impuesto-al-refresco-espiados-con-malware-gubernamental/

191. Disponible en: https://r3d.mx/gobiernoespia/

192. Ver también: Ahmed, Azam & Perlroth, Nicole, "Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families", *The New York Times*, 19 de junio de 2017, disponible en: https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html

- Unonoticias.net
- Univision.click
- Iusacell-movil.com.mx
- Youtube.com.mx
- Fb-accounts.com
- Googleplay-store.com
- Whatsapp-app.com
- smsmensaje.mx

Las organizaciones y personas documentadas recibieron mensajes que pretenden infectar sus dispositivos con el *malware Pegasus* —corroborados con apoyo de *Citizen Lab* de la Universidad de Toronto— incluye a las personas defensoras de derechos humanos Mario Patrón, Stephanie Brewer y Santiago Aguirre, integrantes del Centro de Derechos Humanos Miguel Agustín Pro Juárez, A.C. (*Centro Prodh*); las periodistas de *Aristegui Noticias*: Carmen Aristegui, Rafael Cabrera y Sebastián Barragán; las periodistas Marcela Turati y Carlos Loret de Mola; Salvador Camarena y Daniel Lizárraga; los activistas Juan Pardinas y Alexandra Zapata del Instituto Mexicano para la Competitividad (IMCO); e incluso, un menor de edad, Emilio Aristegui, hijo de la periodista Carmen Aristegui.

Tras el análisis de contexto de las fechas y personas atacadas, se acreditó la existencia de un patrón que vincula la actividad periodística, de combate a la corrupción y de defensa de derechos humanos de las víctimas y la afectación de intereses del gobierno federal.

El 18 de julio de 2021, una investigación denominada *Pegasus Project*, coordinada por *Forbidden Stories* –una organización francesa dedicada al periodismo de investigación–, en conjunto con Amnistía Internacional, en la que participaron más de 80 periodistas del mundo de 17 medios y organizaciones, reveló nueva información sobre la magnitud de los ataques con el *malware Pegasus* en México.

De acuerdo a la información revelada por medios como *Aristegui Noticias*,[193] *Proceso*,[194] *The*

193. "Pegasus Project | Familiares de los 43 normalistas de Ayotzinapa, en la lista de objetivos de espionaje con Pegasus", *Aristegui Noticias*, 18 de julio de 2021, disponible en: https://aristeguinoticias.com/1807/mexico/pegasus-project-familiares-de-los-43-normalistas-de-ayotzinapa-en-la-lista-de-objetivos-del-programa-de-espionaje-pegasus/

194. Tourliere, Mathieu, "Peña Nieto, el desenfrenado espionaje contra periodistas", *Proceso*, 15 de noviembre de 2023, disponible en: https://www.proceso.com.mx/nacional/2021/7/18/pena-nieto-el-desenfrenado-espionaje-contra-periodistas-268034.html

Washington Post,[195] y *The Guardian*,[196] más de 50 mil números de teléfono aparecen como potenciales objetivos de *Pegasus*, de los cuales más de 15 mil poseen el código de país de México. Dentro de los 15 mil números mexicanos reportados, se incluyen los de personas defensoras de derechos humanos, familiares de los 43 estudiantes de la Normal Rural de Ayotzinapa, investigadores de la Comisión Interamericana de Derechos Humanos y de más de 25 periodistas, incluyendo al periodista guerrerense Cecilio Pineda Brito, quien fue asesinado en marzo de 2017, apenas unas semanas después de haber sido atacado con *Pegasus*, según la información publicada.

Inclusive, se ha revelado que un número importante de funcionarios públicos, incluyendo al presidente Andrés Manuel López Obrador, su familia y sus colaboradores también han sido infectados. En respuesta a las revelaciones, el entonces presidente López Obrador e integrantes de su gobierno asumieron públicamente diversos compromisos de transparencia, colaboración con las investigaciones y garantías de no repetición.[197]

Investigaciones periodísticas y de las organizaciones de la sociedad civil han verificado que autoridades mexicanas como SEDENA, el entonces Centro de Investigación y Seguridad Nacional (CISEN) y la entonces Procuraduría General de la República (PGR), mediante la Agencia de Investigación Criminal (AIC), habían comprado este software.[198] Las contrataciones ocurrieron a través de diversas empresas intermediarias como ***Grupo Tech Bull S.A. de C.V.***, ***Proyectos y Diseños VME S.A. de C.V.*** y ***Air Cap S.A. de C.V.***

Estas compañías han sido identificadas como parte del entramado de empresas relacionadas a la empresa *KBH* y al empresario israelí Uri Emmanuel Ansbacher.[199] Los contratos fueron asignados directamente a las empresas, muchas de las cuales resultaron ser empresas fantas-

---

195. Priest, Dana, *et. al.*, "Private Israeli spyware used to hack cellphones of journalists, activists worldwide", *The Washington Post*, 18 de julio de 2021, disponible en: https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/?itid=hp-top-table-main

196. Kirchgaessner, Stephanie, *et. al.*, "Revealed: leak uncovers global abuse of cyber-surveillance weapon", *The Guardian*, 18 de julio de 2021, disponible en: https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus

197. R3D, "Para garantizar el esclarecimiento y la no repetición del espionaje a la sociedad civil es necesario implementar los compromisos asumidos por el Presidente López Obrador", 26 de julio de 2021, disponible en: https://r3d.mx/2021/07/26/para-garantizar-el-esclarecimiento-y-la-no-repeticion-del-espionaje-a-la-sociedad-civil-es-necesario-implementar-los-compromisos-asumidos-por-el-presidente-lopez-obrador/

198. R3D, "Lo que sabemos de las autoridades que adquirieron Pegasus en México", 23 de julio de 2021, disponible en: https://r3d.mx/2021/07/23/autoridades-pegasus-mexico/

199. "Pegasus Project: la red de empresas que vendió Pegasus al gobierno de Peña Nieto", *Aristegui Noticias*, 21 de julio de 2021, disponible en: https://aristeguinoticias.com/2107/mexico/pegasus-project-la-red-de-empresas-que-vendio-pegasus-al-gobierno-de-pena-nieto/

ma, sin experiencia, que utilizaron prestanombres y domicilios falsos.[200] Inclusive, la Unidad de Inteligencia Financiera (UIF) alertó indicios de sobrecostos en las adquisiciones.[201]

iii. Ejército Espía: ataques con Pegasus durante el gobierno de Andrés Manuel López Obrador (2019-2022)

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.[202]

La investigación destaca un documento interno de la SEDENA,[203] obtenido por el Colectivo Guacamaya, que demuestra la celebración de un contrato entre la SEDENA y la empresa ***Comercializadora Antsua*** –designada con los derechos exclusivos para la venta de *Pegasus*– en abril de 2019, cuyo objetivo era la adquisición de un "*Servicio de Monitoreo Remoto de Información*". Es importante reiterar que la SEDENA no cuenta con autorización legal para interceptar comunicaciones privadas de civiles.

Hasta ahora, las víctimas documentadas incluyen el subsecretario de Derechos Humanos, Alejandro Encinas;[204] el 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;[205] una organización de derechos humanos, el Centro de Derechos Humanos Miguel Agustín Pro Juárez (Centro Prodh); el defensor de los derechos humanos Raymundo Ramos, y dos perio-

200. Olmos, R. Durán, V. y Lizárraga, D., "PGR compró *Pegasus* a prestanombres", *Mexicanos contra la Corrupción y la Impunidad*, 28 de julio de 2017, disponible en: https://contralacorrupcion.mx/web/pgrcompropegasus/index.html

201. Rubí, M., "La PGR compró Pegasus a un fantasma", *Mexicanos contra la Corrupción y la Impunidad*, 21 de julio de 2021, disponible en: https://contralacorrupcion.mx/la-pgr-compro-pegasus-a-un-fantasma/

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

203. R3D, *Ejército Espía*, disponible en: https://ejercitoespia.r3d.mx/wp-content/uploads/2022/10/Mortal-de-Oficio.png

204. 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

205. 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/

distas, Ricardo Raphael y un periodista del medio digital *Animal Político*.[206] Las infecciones con *Pegasus* ocurrieron en momentos en que las víctimas realizaban labores relacionadas con violaciones a derechos humanos cometidas por las Fuerzas Armadas.

Por ejemplo, el subsecretario Encinas estaba a cargo de la Comisión de la Verdad por la desaparición de 43 estudiantes de Ayotzinapa, en la que participaron elementos del Ejército. El Centro Prodh representa a las familias de las víctimas en dicho caso y representa a muchas otras víctimas de abusos militares. El *Centro Prodh* también había sido atacado con *Pegasus* durante el gobierno anterior, de abril a junio de 2016.[207] Así mismo, los periodistas fueron agredidos cuando publicaban información relacionada con los abusos contra los derechos humanos cometidos por elementos militares.

La investigación *Ejército Espía* también publicó información que demuestra fehacientemente que el Secretario de la Defensa Nacional, así como otros altos mandos militares, tuvieron conocimiento de una tarjeta informativa que da cuenta de la vigilancia ilegal al defensor Raymundo Ramos realizada con *Pegasus* por la SEDENA, incluyendo sus conversaciones con periodistas en fechas en las que *Citizen Lab* confirmó que su teléfono estaba infectado con *Pegasus*.[208] En esas fechas se publicó un video que mostraba una ejecución extrajudicial por parte del Ejército en Nuevo Laredo, Tamaulipas. Raymundo Ramos asistía en ese momento a los familiares de las víctimas.

Documentos obtenidos de la filtración del colectivo Guacamaya revelaron la estructura militar detrás del uso de *Pegasus*: el **Centro de Inteligencia Militar** (C.M.I.).[209] El C.M.I. es un organismo que formaba parte de la Subjefatura de Inteligencia del Estado Mayor de la Defensa Nacional, brazo operativo de la SEDENA. En otro documento se menciona al C.M.I. como usuario final del "*Sistema de Monitoreo Remoto de Información*" adquirido por la SEDENA a través de *Comercializadora Antsua*, la empresa autorizada para representar exclusivamente a *NSO Group* ante la SEDENA.

---

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

207. Scott-Railton, J., *et al.*, Report: "Reckless Exploit, Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware", *The Citizen Lab*, 19 de junio de 2017, disponible en: https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/

208. R3D: Red en Defensa de los Derechos Digitales, *Ejército Espía*, disponible en: https://ejercitoespia.r3d.mx/wp-content/uploads/2022/10/Mortal-de-Oficio.png
Se destaca la publicación de una tarjeta informativa con carácter secreto, elaborada el 2 de septiembre de 2020 bajo el nombre "Actividades Raymundo Ramos", en la que se da cuenta de las conversaciones que sostuvo el defensor de derechos humanos con periodistas, entre el 16 de agosto y el 26 de agosto de 2020; es decir, exactamente durante las fechas en que el análisis forense de Citizen Lab concluyó que el teléfono de Raymundo Ramos estaba infectado con *Pegasus*.

209. Centro Militar de Inteligencia (SEDENA), "Misión y Objetivo del C.M.I. E.M.D.N.", Mayo 2021, disponible en: https://r3d.mx/wp-content/uploads/MISION-CMI.pdf

iv. Repercusiones internacionales

La gravedad de los hechos denunciados ha motivado el pronunciamiento de organismos internacionales. Por ejemplo, cuatro expertos de las Naciones Unidas emitieron un comunicado en el que enfatizaron el deber de las autoridades mexicanas de garantizar las condiciones necesarias para una investigación transparente, independiente e imparcial sobre las denuncias de la utilización del malware con la intención de espiar a defensores de derechos humanos, activistas y periodistas.[210]

Además, al finalizar su visita conjunta a México, los Relatores para la Libertad de Expresión de la ONU y de la CIDH expresaron su preocupación por el caso y recomendaron asegurar la independencia de la investigación sobre la compra y uso de *malware* (incluyendo *Pegasus*) para vigilar periodistas, activistas y defensores de derechos humanos, así como adoptar medidas legislativas y controles judiciales adecuados para que las medidas de vigilancia se realicen en apego a los derechos humanos. Incluso recomendaron que México debería considerar crear un órgano independiente para supervisar de manera efectiva las tareas de vigilancia del Estado.[211]

En sentido similar, el Relator Especial para Personas Defensoras de Derechos Humanos, Michel Forst, emitió su informe tras su visita al país en 2017, en el que señala que la vigilancia secreta a personas defensoras de derechos humanos es un nuevo y preocupante desafío, especialmente al carecer de medidas adecuadas de control. Respecto a la adquisición de *Pegasus* por parte de las autoridades mexicanas y su aparente uso para vigilar a periodistas y personas defensoras, reiteró su llamamiento y el de otros expertos de las Naciones Unidas para que se lleve a cabo una investigación independiente e imparcial sobre la presunta vigilancia ilegal, al constituir una grave violación de los derechos a la privacidad y las libertades de expresión y asociación.[212]

Ante la nueva evidencia de la continuación del espionaje por parte de las fuerzas armadas, la CIDH reiteró su preocupación en junio de 2023, instando al Estado mexicano a investigar y sancionar a los responsables y a cesar inmediatamente la venta, transferencia y uso de este

---

210. Alto Comisionado de las Naciones Unidas para los Derechos Humanos, "México: expertos de la ONU piden investigación independiente e imparcial sobre el uso de spyware contra defensores de DDHH y periodistas", Comunicado de prensa, 19 de julio de 2017, disponible en: http://www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?-NewsID=21892&LangID=S

211. Observaciones preliminares del Relator Especial de la ONU sobre la libertad de expresión y el Relator Especial sobre libertad de expresión de la CIDH después de su visita conjunta en México, 27 de noviembre – 4 de diciembre 2017, disponible en: https://www.oas.org/es/cidh/expresion/docs/Observaciones_Preliminares_ESP.PDF

212. Informe del Relator Especial sobre la situación de los defensores de los derechos humanos relativo a su misión a México, 12 de febrero de 2018, A/HRC/37/51/Add.2, disponible en: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session37/Pages/ListReports.aspx

tipo de tecnologías hasta que se establezcan marcos normativos apegados a los estándares de derechos humanos.[213] Por su parte, un grupo de Relatores Especiales de la Organización de las Naciones Unidas también expresaron su preocupación al gobierno mexicano por el uso del *malware Pegasus* para vigilar a personas defensoras de derechos humanos.[214]

Así mismo, en el marco del cuarto ciclo del Examen Periódico Universal (EPU) del Consejo de Derechos Humanos de las Naciones Unidas, el gobierno de México recibió recomendaciones puntuales por parte de Costa Rica y Países Bajos acerca de la vigilancia ilegal cometida en el país en contra de periodistas y personas defensoras de derechos humanos.[215]

v. Encubrimiento, opacidad e impunidad

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

A pesar del llamado de múltiples instancias, nacionales e internacionales –como la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OACNUDH)[216] y los Procedimientos Especiales de la ONU, la Comisión Interamericana de Derechos Humanos

213. Comisión Interamericana de Derechos Humanos, "CIDH manifiesta su preocupación por el aumento de casos sobre uso de Pegasus en México", Comunicado de Prensa, 2 de junio de 2023, disponible en: https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/prensa/comunicados/2023/109.asp

214. Mandatos de la Relatora Especial sobre la situación de los defensores de derechos humanos; del Grupo de Trabajo sobre la cuestión de los derechos humanos y las empresas transnacionales y otras empresas; de la Relatora Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión; del Relator Especial sobre los derechos a la libertad de reunión pacífica y de asociación y de la Relatora Especial sobre el derecho a la privacidad, 21 de junio de 2023, Ref.: AL MEX 3/2023, disponible en: https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=28131

215. R3D: Red en Defensa de los Derechos Digitales, "Examen Periódico Universal: Costa Rica y Países Bajos piden a México investigar y sancionar la vigilancia ilegal", 24 de enero de 2024, disponible en: https://r3d.mx/2024/01/24/examen-periodico-universal-costa-rica-y-paises-bajos-piden-a-mexico-investigar-y-sancionar-la-vigilancia-ilegal/

216. Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, "La ONU-DH expresa su preocupación por actos de vigilancia ilícita contra personas defensoras de derechos humanos y periodistas", 11 de octubre de 2022, disponible en: https://hchr.org.mx/comunicados/la-onu-dh-expresa-su-preocupacion-por-actos-de-vigilancia-ilicita-contra-personas-defensoras-de-derechos-humanos-y-periodistas/

(CIDH)[217]– sobre la necesidad de llevar a cabo una investigación diligente, con garantías de autonomía reforzadas, más de siete años después de la primera denuncia y a dos años del inicio de la segunda investigación, no han existido avances significativos.

La única detención de una persona,[218] a quien se le imputó el delito de intervención telefónica por su probable participación como operador del software dentro de una de las empresas intermediarias entre *NSO Group* y la PGR, solo fue posible gracias a información proporcionada por una de las víctimas, que remitió a las autoridades a la red de intermediarios que operaba *Pegasus*.

En el juicio llevado en contra de dicho operador en diciembre de 2023, se confirmó mediante sentencia judicial la ilegal intervención de comunicaciones en contra de la periodista Carmen Aristegui, sin embargo, la persona acusada fue dejada en libertad ante la falta de elementos para demostrar su participación directa en dicho espionaje.

Tampoco han existido avances en la imputación de responsabilidades de autoridades e instituciones. Por el contrario, la Fiscalía, entre otras deficiencias, se ha negado a realizar actos esenciales de investigación, ha obstruido y fragmentado las investigaciones, ha hecho recaer la carga de la prueba en las víctimas y les ha negado copia de los expedientes.[219] La justicia y la rendición de cuentas también son obstruidas por las autoridades denunciadas, quienes afirman sistemáticamente que no existe ninguna base de datos o documentación formal de los registros relativos a las personas o números atacados.

En 2019, el Instituto Nacional de Acceso a la Información y Protección de Datos Personales (INAI) determinó que la Fiscalía había incumplido sus obligaciones conforme a la legislación de Protección de Datos Personales al ocultar contratos con *NSO Group*.[220] Sin embargo, hasta

217. Relator Especial de las Naciones Unidas (ONU) para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA, "Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expression", 21 de junio de 2013, disponible en: https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=926&lID=2

218. "Avance del caso Pegasus en México debe ser un punto de no retorno que ayude a esclarecer un crimen de talla mundial", *Article 19 MX-CA*, 8 de noviembre de 2021, disponible en: https://articulo19.org/avance-del-caso-pegasus-en-mexico-debe-ser-un-punto-de-no-retorno-que-ayude-a-esclarecer-un-crimen-de-talla-mundial/%20; "Detiene FGR a uno de los involucrados en espionaje con Pegasus", *Aristegui Noticias*, 8 de noviembre de 2021, disponible en: https://aristeguinoticias.com/0811/mexico/detiene-fgr-a-uno-de-los-involucrados-en-espionaje-con-pegasus/

219. Carpeta de investigación FEADLE FED/SDHPDSC/UNAI-CDMX/0000430/2017; Ahmed, Azam, "Mexico Spyware Inquiry Bogs Down. Skeptics Aren't Surprised", *The New York Times*, 20 de febrero de 2018, disponible en: https://www.nytimes.com/2018/02/20/world/americas/mexico-spyware-investigation.html; R3D: Red en Defensa de los Derechos Digitales, "A un año de #GobiernoEspía, prevalece la impunidad", 20 de junio de 2018, disponible en: https://r3d.mx/2018/06/20/comunicado-a-un-ano-de-gobiernoespia-prevalece-la-impunidad/

220. INAI, "Determina INAI que FGR, respecto al software Pegasus, incumplió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados", 20 de febrero de 2019, disponible en: https://inicio.inai.org.mx/Comunicados/Comunicado%20INAI-054-19.pdf

la fecha, la FGR se ha negado a emprender cualquier investigación seria e independiente en relación con la obstrucción de la justicia documentada.

La renuencia de la Fiscalía a realizar diligencias en cuanto a líneas de investigación respecto de la AIC de la Fiscalía General demuestra la falta de autonomía, imparcialidad y profesionalismo en la investigación, máxime cuando tanto la autoridad que realiza la investigación (la FEADLE), como la única autoridad que ha admitido el uso del *malware Pegasus* (la AIC) forman parte de la misma Fiscalía General. Así mismo, no se han llevado a cabo acciones de investigación serias respecto al CISEN ni al Ejército Mexicano, pese a las evidencias que los confirman como operadores de *Pegasus* durante el gobierno pasado.

A pesar de las promesas de la Presidencia de la República, la SEDENA ha emprendido una estrategia de ocultamiento de información sobre las contrataciones relacionadas al *spyware Pegasus*, así como respecto de la existencia misma del Centro Militar de Inteligencia.

Inicialmente, la SEDENA negó la existencia de contratos con *Comercializadora Antsua*. Sin embargo, frente a evidencia de su existencia entregada a la Auditoría Superior de la Federación (ASF) y obtenida por R3D, el INAI resolvió revocar la respuesta de inexistencia y ordenó la entrega de la información solicitada.[221] Dicha resolución inatacable no ha sido cumplida, incluso a pesar de que un juez de distrito ya ha concedido un amparo para su cumplimiento.[222] La información sobre las contrataciones incluso ha sido negada a la FGR, quien la ha solicitado como parte de sus investigaciones.

Por otra parte, la SEDENA ha pretendido negar la existencia del Centro Militar de Inteligencia, a pesar de que en agosto de 2022, la Presidencia de la Comisión para la Verdad del Caso Ayotzinapa (COVAJ) presentó su primer informe,[223] donde refirió documentos sobre intervenciones de comunicaciones de la SEDENA, con las siglas C.M.I. en la parte superior derecha.

Al respecto, el Grupo Interdisciplinario de Expertos Independientes (GIEI) preguntó a la SEDENA sobre el significado de las siglas C.M.I. que aparecían en los documentos de inteligencia. La Secretaría respondió que las siglas correspondían a la frase "*contenido mediático de información*".

---

221. R3D: Red en Defensa de los Derechos Digitales. "SEDENA debe entregar toda la información sobre contratos con proveedora de Pegasus", 26 de enero de 2023, disponible en: https://r3d.mx/2023/01/26/sedena-debe-entregar-toda-la-informacion-sobre-contratos-con-proveedora-de-pegasus/

222. R3D: Red en Defensa de los Derechos Digitales. "Juez ordena a la SEDENA cumplir resolución del INAI que le obliga a entregar contratos de Pegasus", 23 de julio de 2024, disponible en: https://r3d.mx/2024/07/23/juez-ordena-a-la-sedena-cumplir-resolucion-del-inai-que-le-obliga-a-entregar-contratos-de-pegasus/

223. Informe de la Presidencia de la Comisión para la Verdad y Acceso a la Justicia del Caso Ayotzinapa, disponible en: https://comisionayotzinapa.segob.gob.mx/es/Comision_para_la_Verdad/Informe_Presidencia

La SEDENA también ha dado respuestas discordantes a los familiares de los 43 estudiantes normalistas de Ayotzinapa. En agosto de 2023, las familias –acompañadas jurídicamente por el *Centro Prodh*– presentaron una demanda de amparo por la obstaculización del Ejército en las indagatorias del caso y solicitaron una suspensión provisional para evitar la destrucción de documentos.[224]

En esta demanda de amparo, los familiares nombraron al Centro Militar de Inteligencia como una de las autoridades responsables. Dentro del juicio, la SEDENA negó la existencia actual del C.M.I., pero reconoció que sí existió al decir que "*fue creado como un organismo circunstancial, pero a la fecha ha cesado sus funciones*".

Además, al pretender dar cumplimiento a una resolución del INAI que le ordena entregar información sobre el C.M.I., la SEDENA volvió a negar su existencia, alegando que "*no existe ni existió un área, departamento u oficina denominada 'Centro Militar de Inteligencia' o con denominación análoga*".

Sin embargo, la existencia del C.M.I. se encuentra reconocida en documentos públicos de la SEDENA. Por ejemplo, en el Segundo Informe de Labores de la SEDENA,[225] públicamente disponible en el sitio web de la dependencia, se menciona una Reunión de Alto Nivel, sostenida el 24 de septiembre de 2019 en las instalaciones del Centro Militar de Inteligencia (C.M.I.).

La burda estrategia de ocultamiento por parte del ejército y la Presidencia de la República ha sido exitosa, en tanto se continúa ocultando información y obstaculizando las investigaciones sobre el espionaje militar ilegal con *Pegasus*. A su vez, México no ha aceptado el establecimiento de un mecanismo internacional de supervisión o investigación independiente y los documentos relacionados con la contratación y uso de *Pegasus* aún no han sido hechos públicos por las autoridades del Estado mexicano. El gobierno no solo ha faltado a su obligación de garantizar la verdad y justicia a las víctimas, sino que ha perpetuado la impunidad y generado las condiciones para la repetición de los hechos.

d. Reign de Quadream

QuaDream Ltd es una empresa israelí especializada en el desarrollo y venta de avanzada tecnología de ofensiva digital vendida a clientes gubernamentales. A pesar de que la empresa opera con una presencia pública mínima, carece de sitio web, cobertura mediática o presencia en las redes sociales, es conocida por un *spyware* comercializado bajo el nombre de ***Reign***.

---

224. "#Comunicado | Poder Judicial ordena al Ejército no destruir documentos del caso #Ayotzinapa", *tweet* de @CentroProdh, disponible en: https://twitter.com/CentroProdh/status/1698389347462988123

225. Segundo Informe de Labores de la Secretaría de la Defensa Nacional, 2019-2020, 1 de septiembre de 2020, disponible en: https://transparencia.sedena.gob.mx/pdf/Informe_de_Labores_2019-2024/2do_Informe_de_Labores_2019-2024.pdf

Un reporte de *Citizen Lab*, en colaboración con *Microsoft Threat Intelligence*, detectó un nuevo *spyware* en México y nueve países más, comercializado por *QuaDream*, conocido como *Reign* y que opera de manera similar a *Pegasus*, entre otras características, al no ser necesario que el usuario haga clic para que el malware infecte dispositivos.[226]

De acuerdo con el reporte, una vulnerabilidad denominada *Endofdays* fue explotada en las versiones de *iOS* 14.4 y 14.4.2 y, posiblemente, en otras versiones para instalar el *spyware* en los dispositivos de las víctimas mediante el uso de invitaciones de calendario invisibles de *iCloud* enviadas por *QuaDream*.

El *spyware* puede grabar llamadas telefónicas y audio desde el micrófono; tomar fotografías a través de la cámara frontal y trasera del dispositivo; filtrar y eliminar elementos del llavero del dispositivo; ejecutar consultas en bases de datos SQL en el teléfono; limpiar los restos que podrían quedar atrás por las vulnerabilidades de cero clics; hacer seguimiento de la ubicación del dispositivo; y realizar varias operaciones del sistema de archivos.

Entre las víctimas detectadas alrededor del mundo, en un periodo entre finales de 2021 y principios de 2023, se incluyen periodistas, opositores políticos y organizaciones no gubernamentales. Además de otros países como Singapur, Arabia Saudita y Ghana, en 2022, Meta le atribuyó actividad dentro de su plataforma, incluyendo el uso de alrededor de 250 cuentas para probar las capacidades del *spyware* en dispositivos iOS y Android.[227]

De acuerdo a *Citizen Lab*, los empleados de *QuaDream* han recibido instrucciones de abstenerse de mencionar a su empleador en las redes sociales. Sin embargo, a través de una revisión de la documentación corporativa, artículos de prensa y bases de datos, *Citizen Lab* ha podido identificar a varias figuras clave relacionadas con la empresa, incluidos sus tres fundadores: Ilan Dabelstein, Guy Geva y Nimrod Rinsky.[228]

De igual forma, documentos judiciales de un litigio entre *QuaDream* e *InReach* –otra empresa registrada en Chipre con el único propósito de promover los productos de *QuaDream* fuera de

226. Marczak, Bill, et. al.,"A First Look at Spyware Vendor QuaDream's Exploits, Victims, and Customers", *The Citizen Lab*, 11 de abril de 2023, disponible en: https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/

227. Dvilyanski, Mike, et. al, "Threat Report on the Surveillance-for-Hire Industry", *Meta*, 15 de diciembre de 2022, disponible en: https://about.fb.com/wp-content/uploads/2022/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf

228. Marczak, Bill, *et. al.*,"A First Look at Spyware Vendor QuaDream's Exploits, Victims, and Customers", *The Citizen Lab*, 11 de abril de 2023, disponible en: https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/

Israel– han permitido saber que *QuaDream* vendía sus productos fuera de Israel a través de la misma, sin que necesariamente fuera su distribuidora exclusiva o principal.

De acuerdo con medios de comunicación como *Globes*, el sistema de *Quadream* es sustancialmente más barato que el de *NSO Group* y no está sujeto al control reglamentario del Ministerio de Defensa israelí.[229]

B. Herramientas de extracción forense

Otras tecnologías de intervención de comunicaciones detectadas en México 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 estos.

Mediante el uso de estos escáneres forenses es posible tener acceso a registros de llamadas, mensajes de texto (SMS), imágenes, vídeos, archivos de audio, información de números de identificación como ESN IMEI, ICCID e IMSI de dispositivos móviles. Además, permite la clonación de chips, extracción de contraseñas, recuperación de información borrada e inclusive en algunos casos permite conocer el contenido de aplicaciones de mensajería como *WhatsApp, iMessage*, entre otras.

Las herramientas de extracción forense pueden ser fácilmente abusadas para vigilar a personas de manera injustificada y su uso legítimo en investigaciones criminales como un medio de obtención de evidencia puede ser manipulable. Por ejemplo, el ex director ejecutivo de *Signal*, Moxie Marlinspike, expuso diversas vulnerabilidades en el software de los escáneres que permiten manipular la información obtenida.[230] Esta información puede ser después utilizada para incriminar a personas de manera injustificada en juicios legales o procesos administrativos.[231]

La empresa israelí ***Cellebrite*** es la desarrolladora de la herramienta de extracción forense más popular en México y en el mundo. Por años se ha documentado la comercialización de estos

229. Gilead, Assaf, "NSO rival Quadream in talks with Moroccan gov't", *Globes*, 10 de agosto de 2021, disponible en: https://en.globes.co.il/en/article-nso-rival-quadream-in-talks-with-moroccan-govt-1001381146

230. R3D, "Director de Signal expone vulnerabildiad en el equipo de hacking Cellebrite", 23 de abril de 2021, disponible en: https://r3d.mx/2021/04/23/director-de-signal-expone-vulnerabilidad-en-el-equipo-de-hacking-cellebrite/

231. Marlinspike, Moxie, "Exploiting vulnerabilities in Cellebrite UFED and Physical Analyzer from an app's perspective", *Signal*, 21 de abril de 2021, disponible en: https://signal.org/blog/cellebrite-vulnerabilities/

productos a decenas de gobiernos, incluyendo regímenes autocráticos u opresivos de países como China, Turquía, Venezuela, Bielorrusia, Rusia y Bangladés, los cuales han utilizado dichos equipos para vigilar injustificadamente a disidentes, periodistas, activistas, personas de la comunidad LGBTQI y personas pertenecientes a minorías étnicas.[232]

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.[233] Los casos en los que ha actuado ante violaciones han sido hasta que estos llegan a los medios o hasta que son obligados a abordarlos a partir de procesos legales.[234]

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.

Solicitudes de acceso a la información realizadas por R3D e investigaciones periodísticas de medios como *Animal Político* han permitido detectar la adquisición de estas tecnologías por las siguientes autoridades:

232. Krapiva, Natalia & Hinako, "What spy firm Cellebrite can't hide from investors", *Access Now*, 26 de mayo de 2021 (actualizado el 13 de enero de 2023), disponible en: https://www.accessnow.org/what-spy-firm-cellebrite-cant-hide-from-investors/

233. "I Worked at Israeli Phone Hacking Firm Cellebrite. They Lied to Us", *Haaretz*, 27 de julio de 2021, disponible en: https://www.haaretz.com/israel-news/i-worked-at-israeli-phone-hacking-firm-cellebrite-they-lied-to-us-1.10041753

234. Dhali, Bari, "Israeli phone-hacking firm Cellebrite to stop sales to Bangladesh", *Dhaka Tribune*, 18 de agosto de 2021, disponible en: https://www.dhakatribune.com/world/2021/08/18/israeli-phone-hacking-firm-cellebrite-to-stop-sales-to-bangladesh

Entidad	Institución	Herramienta
Federal	Secretaría de la Defensa Nacional	Cellebrite – UFED 4PC
Federal	Instituto Nacional de Migración	Cellebrite
Federal	Fiscalía General de la República	Cellebrite – UFED Touch 2
Aguascalientes	Policía Cibernética de Aguascalientes	Cellebrite – UFED 4PC
Aguascalientes	Secretaría de Seguridad Pública de Aguascalientes	Cellebrite – UFED 4PC
Baja California Sur	Procuraduría General de Justicia del Estado de Baja California Sur	Cellebrite – UFED 4PC
Baja California Sur	Procuraduría General de Justicia del Estado de Baja California Sur	MAGNET AXIOM
Baja California Sur	Secretaría de Seguridad Pública de Baja California Sur	Cellebrite – UFED 4PC
Campeche	Fiscalía General del Estado de Campeche	Cellebrite – UFED 4PC
Campeche	Secretaría de Protección y Seguridad Ciudadana de Campeche	MSAB – XRY
Chiapas	Fiscalía General de Justicia del Estado de Chiapas	Cellebrite – UFED Touch Ultimate
Chihuahua	Secretaría de Seguridad Pública del Estado de Chihuahua	Digital Intelligence – FRED
Chihuahua	Fiscalía General del Estado de Chihuahua	Cellebrite –UFED TOUCH 2, UFED 4 PC ULTIMATE, UFED 2 TOUCH ULTIMATE MAGNET AXIOM
Ciudad de México	Secretaría de Seguridad Ciudadana de la Ciudad de México	Cellebrite – UFED 4PC
Estado de México	Fiscalía General de Justicia del Estado de México	Cellebrite – UFED Touch 2

Tabla 3.5.a. Autoridades mexicanas que adquirieron tecnologías de Cellebrite. Solicitudes de acceso a la información e investigaciones periodísticas.

Entidad	Institución	Herramienta
Guanajuato	Fiscalía General del Estado de Guanajuato	Cellebrite – UFED TOUCH 2, UFED 4 PC ULTIMATE, UFED 2 TOUCH ULTIMATE MAGNET AXIOM Digital Intelligence – FRED DX 2 RAID
Hidalgo	Procuraduría General de Justicia de Hidalgo	Cellebrite – UFED TOUCH 2, UFED 4 PC
Hidalgo	Secretaría de Seguridad Pública de Hidalgo	Cellebrite – UFED TOUCH 2, UFED 4 PC
Jalisco	Instituto Jaliscience de Ciencias Forenses de Jalisco	Cellebrite – UFED 4 PC
Michoacán	Fiscalía General del Estado de Michoacán	Cellebrite – UFED 4 PC
Nuevo León	Fiscalía General de Justicia de Nuevo León	Cellebrite – UFED 4 PC
Querétaro	Fiscalía General del Estado de Querétaro	Cellebrite – UFED Touch 2
Quintana Roo	Fiscalía General del Estado de Quintana Roo	Cellebrite – UFED Touch 2
Sinaloa	Comisión Estatal de Búsqueda de Personas de Sinaloa	Cellebrite – UFED 4 PC
Sinaloa	Fiscalía General del Estado de Sinaloa	Cellebrite – UFED 4 PC
Tabasco	Fiscalía General del Estado de Tabasco	Cellebrite
Yucatán	Fiscalía General de Justicia del Estado de Yucatán	Cellebrite – UFED Touch 2

Tabla 3.5.b. Autoridades mexicanas que adquirieron tecnologías de Cellebrite. Solicitudes de acceso a la información e investigaciones periodísticas.

No solamente se aprecia la utilización de este tipo de tecnologías por parte de autoridades sin facultades para la intervención de comunicaciones privadas, como el Instituto Nacional de Migración (INM) o la SEDENA, sino que existen indicios de utilización ilegal por parte de las Fiscalías, las cuales –en respuesta a solicitudes de acceso a la información o en la publicación de información en la Plataforma Nacional de Transparencia– han reportado información in-

consistente; en ocasiones, indicando no haber solicitado autorización judicial para la extracción de información ni una sola vez, a pesar de gastar millones de pesos en adquirir equipo con esos fines.

C. Vigilancia masiva con antenas falsas

La red de telefonía móvil se compone en gran medida de antenas –también llamadas estaciones base– y conmutadores, que sirven como "puentes" entre las antenas y el resto de la red de telefonía móvil. Las antenas de telefonía móvil están distribuidas a lo largo y ancho del país.

Las **antenas falsas** (también conocidas como *IMSI catchers* o *stingrays*) son dispositivos que engañan a los teléfonos móviles, haciéndoles creer que son antenas legítimas para recolectar información en un radio determinado y de forma encubierta. Al posicionarse como receptores y transmisores de la señal de telefonía móvil, engañan, por un lado, a los dispositivos —al hacerse pasar por una antena perteneciente a algún proveedor de telefonía móvil— y, por otro, a una antena legítima haciéndose pasar por el o los dispositivos que buscan conectarse con la red de telefonía móvil.[235]

Para atraer dispositivos dentro de su rango, las antenas falsas se posicionan como la señal más fuerte dentro del vecindario de antenas. Una vez que las antenas atraen de manera exitosa a los dispositivos en la región, les solicitan que se identifiquen otorgando los números de identificación IMSI, IMEI y su localización aproximada. Para mantener cautivos a los dispositivos que se conectan a la antena falsa, esta les comunica que es la única antena "legítima" en el vecindario. Con esto, los dispositivos se mantendrán conectados a la antena falsa hasta que salgan del rango de señal o se apaguen.

Sobre este punto, es importante enfatizar que la imposición del protocolo GSM (G2) mediante el uso de antenas falsas pone en peligro la privacidad y seguridad de las comunicaciones puesto que dicho protocolo cuenta con débiles protecciones de cifrado,[236] lo que deja sumamente vulnerable el contenido de las comunicaciones en caso de que sean intervenidas.

---

235. Strobel, D., "IMSI Catcher. Ruhr-Universität Bochum", 13 de julio de 2007, disponible en: https://web.archive.org/web/20200807000022/https://www.emsec.ruhr-uni-bochum.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf pg. 7.

236. Según un artículo publicado en la revista *Ars Technica*, solo es necesario contar con conocimientos básicos de programación, una computadora, software libre, cuatro celulares con costo de quince dólares y tres minutos, para poder romper el cifrado presente en las comunicaciones mediante el protocolo GSM. Borland, Jon, "$15 phone, 3 minutes all that's needed to eavesdrop on GSM call", 29 de diciembre de 2018, disponible en: https://arstechnica.com/gadgets/2010/12/15-phone-3-minutes-all-thats-needed-to-eavesdrop-on-gsm-call/

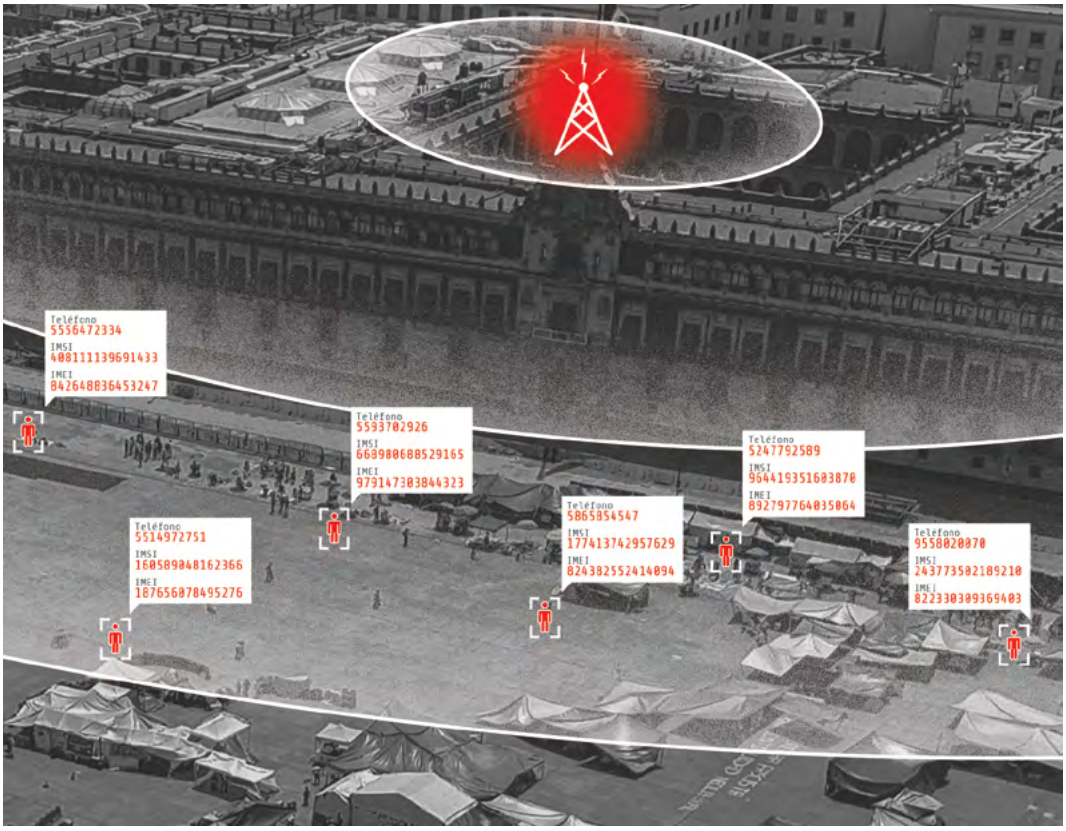


Gráfico 3.2. Funcionamiento de la antena falsa para el rastreo de teléfonos móviles. Ilustración.

Su capacidad de intromisión varía dependiendo del modelo. Algunos, en combinación con otras herramientas de vigilancia, son capaces de interceptar llamadas y mensajes, acceder a los datos y metadatos de las comunicaciones, así como proporcionar la ubicación en tiempo real del dispositivo.[237] Generalmente, las antenas falsas posibilitan conocer el número IMSI, IMEI, el contenido de llamadas y de mensajes SMS, e inclusive tener acceso a archivos contenidos dentro de los dispositivos que se encuentran dentro de su rango.

Las antenas falsas también pueden aparentar ser un dispositivo de comunicación[238] o actuar de manera anónima para enviar mensajes SMS y realizar llamadas. Es conocido que esta fun-

237. *Ibid*.

238. Swingler, S., "Meet the Grabber: How governments and criminals can spy on you (and how to protect yourself)", *Daily Maverick*, 1 de septiembre de 2016, disponible en: https://www.dailymaverick.co.za/article/2016-09-01-meet-the-grabber-how-government-and-criminals-can-spy-on-you-and-how-to-protect-yourself/

ción se ha utilizado para infectar con *malware* a dispositivos[239] y para intimidar a asistentes de protestas. Además de permitir el ejercicio de vigilancia, las antenas falsas también pueden ser utilizadas para bloquear la comunicación de los dispositivos que se conectan a estas.[240]

A partir de la información que puede ser obtenida mediante el uso de antenas falsas se puede derivar el conocimiento de hábitos, preferencias religiosas, sexuales, condiciones de salud, relaciones personales y otros datos que permiten la construcción de detallados perfiles de las personas vigiladas. El simple hecho de tener acceso a este tipo de información atenta en contra del derecho a la privacidad de las personas y las pone en peligro. La retención de estos datos aumenta el peligro de que sean abusados por autoridades y por otros entes en caso de que sean comprometidos.

Aunque no existe un marco legal que regule la utilización de antenas falsas en México, se ha documentado la adquisición de este tipo de sistemas de vigilancia por parte de varias autoridades. Según dos notas periodísticas publicadas en 2015 y 2016, la empresa finlandesa *Exfo Inc.*[241] y la suiza *SECO*[242] vendieron antenas falsas de comunicación a autoridades del Estado mexicano. Hasta ahora, en ninguno de estos dos casos ha sido posible saber qué agencias fueron las que adquirieron el equipo.

Mediante una serie de solicitudes de acceso a la información pública realizadas por R3D, se ha documentado la compra de antenas falsas por parte de diversas autoridades, aunque es razonable suponer que su adquisición y uso es mucho más amplio.

239. Doctorow, C., "Stingray for criminals: spreading mobile malware with fake cellphone towers", *Boing boing*, 29 de marzo de 2017, disponible en: https://boingboing.net/2017/03/29/democratizing-crime.html

240. Israel, T. y C. Parsons, "Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada", Ver. 2, *The Citizen Lab*, agosto de 2016, disponible en: https://citizenlab.ca/wp-content/uploads/2016/09/20160818-Report-Gone_Opaque.pdf pg. 10.

241. Godoy, E., "Finlandia: México le compra equipo para espiar en celulares", *Proceso*, 29 de julio de 2015, disponible en: http://www.proceso.com.mx/449165/finlandia-mexico-le-compra-equipo-espiar-en-celulares

242. Godoy, E., "Suiza también vendió a México equipo de espionaje para celulares", *Proceso*, 8 de agosto de 2016, disponible en: http://www.proceso.com.mx/450175/suiza-exporto-a-mexico-equipo-espionaje-celulares

Autoridad	Proveedor	Folio del contrato	Año	Objeto	Marca	Monto
Procuraduría General de Justicia del Estado de Baja California	Eyetech Solutions S.A. de C.V.	DAD-ADQ-PGJ E-39-15	2015	A. Dos sistemas LTE en módulo para el equipo Engage Gi2. B. Un sistema Engage Pi2.	Verint	$38.793.103,45
		DAD-ADQ-PGJ E-113-16	2016	A. Dos equipos Engage Gi2 – M	Verint	$13.793.103,44
Procuraduría General de Justicia de la Ciudad de México	Eyetech Solutions S.A. de C.V.	PGJDF-173/201 6	2016	A. Un equipo Engage Gi2	Verint	$25.520.000,00
Fiscalía General de Justicia del Estado de México[243]	Acumen Telecomuni caciones, S.A. de C.V.	CB/199/2014	2014	A. Tres equipos Engage Gi2-M	Verint	$62.345.538,60
Fiscalía General de Justicia del Estado de Morelos	Eyetech Solutions S.A. de C.V.	SSP/0195-JM/2 014	2014	A. Un equipo Engage Gi2. B. Un sistema Engage Pi2.	Verint	$46.255.000,00
Fiscalía General del Estado de Nayarit	Neolinx de México, S.A. de C.V.	098/2019	2019	Adquisición de equipo matrix catcher imsi catcher 25 watts	Matrix-Catcher	$46.255.000,00
Procuraduría de Justicia del Estado de Quintana Roo	Rohde & Schwartz de México, S. de R.L. de C.V.	FGE/FASP/004/ 2017	2017	A. Un equipo "GAXG"	Rhode & Schwarz	$14.750.000,00
	Neolinx de México, S.A. de C.V.	FGE/FASP/006/ 2017	2017	NA	NA	$1.900.000,00
Procuraduría General de Justicia del Estado de Puebla	Neolinx de México, S.A. de C.V.	DABS/GESAD-0 66/CECSNSP/11 3/2019	2019	SISTEMA DE CAPTURA DE IDENTIDAD SUSCRIPTOR MÓVIL	Matrix-Catcher	$15.560.334,82

Tabla 3.6. Autoridades mexicanas que han adquirido antenas falsas. Solicitudes de acceso a la inormación.

243. Equipo adquirido por conducto de la Secretaría de Finanzas del Estado de México.

Adicionalmente, documentos internos de la SEDENA revelan la adquisición y uso de antenas falsas de marca *Verint*, Modelo *Engage Pi2*, también denominado por el Ejército como "*Sistema GSM Pasivo*".

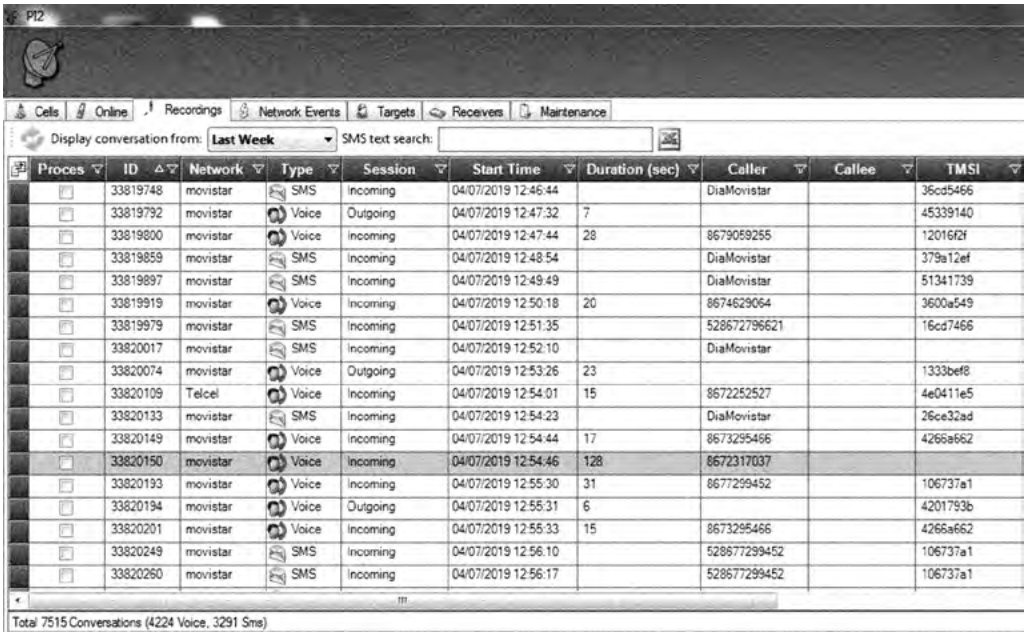


Gráfico 3.3. Producción del Sistema GSM Pasivo. Captura de pantalla.

Las antenas falsas más utilizadas por las autoridades mexicanas son fabricadas por la empresa estadounidense ***Verint,*** fundada en 1994, que se dedica al desarrollo de soluciones de inteligencia y que, según su código de conducta, se adhiere a las leyes concernientes de los países en los que vende equipo, especialmente cuando sus clientes son gobiernos.[244]

244. Verint, Verint Code of Conduct, 2012, disponible en: https://r3d.mx/wp-content/uploads/verint_code_of_conduct.pdf. Pg 30.

a. Sistema Engage Gi2

El **sistema *Gi2***[245] es una antena falsa de celular portátil que cabe en un maletín. A partir de una presentación de la empresa ***Verint***[246] es posible conocer el funcionamiento del equipo y las capacidades de vigilancia y disrupción de comunicación que esta antena falsa confiere.

Gráfico 3.4. Sistema Engage Gi2 de Verint. Dossier de presentación.

Para vigilar dispositivos, el sistema de antena falsa *Gi2* comienza interrogando a una o más de las antenas legítimas que se encuentran dentro de su rango para obtener información sobre la composición del vecindario de antenas. A través de esta interrogación, la antena falsa adquiere conocimiento sobre las antenas disponibles en la región y sobre la frecuencia, potencia y números de identificación de estas.

La información obtenida mediante la interrogación es entonces utilizada para configurar el código de país, el código de la red (o de la empresa de telecomunicaciones) y la potencia de la antena falsa, así como el número de antenas que componen el vecindario, el número de identificación del vecindario, entre otros datos. Esta configuración permite a la antena falsa posar como una antena legítima para pasar desapercibida. Mediante la definición del número de antenas que componen el vecindario se puede mantener a los dispositivos cautivos en la señal de la antena falsa.

245. Verint, Tactical Off- Air Intelligence Solutions, 2013, disponible en: https://r3d.mx/wp-content/uploads/1278-verint-product-list-engage-gi2-engage-pi2.pdf

246. Verint, Verint GI2: Gi2 Features, 2010, disponible en: https://r3d.mx/wp-content/uploads/Gi2.pdf

Una vez que la antena falsa *Gi2* captura dispositivos es posible:

- Obtener números de identificación IMEI, IMSI de los dispositivos.
- Conocer la distancia a la que se encuentran los dispositivos.
- Conocer la localización en coordenadas de los dispositivos.
- Interceptar SMS (entrantes y salientes).
- Enviar SMS falsos (desde el/los dispositivo capturado y hacia el dispositivo capturado).
- Editar SMS (entrantes y salientes).
- Interceptar llamadas (entrantes y salientes). Las llamadas escuchadas son grabadas.
- Realizar llamadas falsas (desde o hacia el/los dispositivos capturados).
- Conocer los números de teléfono de los mensajes y llamadas (entrantes y salientes).
- Prender el micrófono de los dispositivos para escuchar.
- Degradar el protocolo de 3G o 4G a GSM.
- Descifrar cifrado A5/1 y A5/2 (presentes en protocolo GSM).
- Bloquear la comunicación de los dispositivos.

La información obtenida mediante el sistema es guardada en una base de datos en el sistema que permite que ser analizada, hacer referencias cruzadas, ordenarla, entre otras cosas.

b. Sistema LTE para GI2

El **Sistema LTE para *Gi2*** es un suplemento que permite detectar y vigilar dispositivos de nueva generación que se encuentran fuera del alcance del equipo Gi2, que solamente funcionaba para vigilar dispositivos que utilizan el protocolo GSM. Mediante este equipo es posible vigilar dispositivos que utilicen el estándar de la banda LTE, que conforma parte de los protocolos 3G y 4G, mismo que en México cuenta con mayor cobertura.

c. Sistema Pasivo de Rastreo y Análisis de comunicaciones Engage Pi2

Las capacidades de esta antena falsa fueron conocidas mediante un contrato celebrado entre la Procuraduría General de Justicia del Estado de Baja California y la empresa *Eyetech Solutions S.A. de C.V.*[247] y un folleto de la marca *Verint*.[248]

La antena falsa *Pi2* permite:

- Intervenir de manera simultánea 50 llamadas.
- Interceptar mensajes SMS y llamadas de voz.
- Obtener los números de identificación IMEI, IMSI.
- Conocer la ubicación geográfica en tiempo real de los dispositivos intervenidos.
- Interrogar y monitorear a cientos de antenas legítimas.
- Crear un mapa en el que se muestra la ubicación de las antenas legítimas.
- Descifrar cifrado A5/1 y A5/2 (presentes en protocolo GSM).
- Obtener notificaciones cuando alguno de los dispositivos vigilados se conectan, desconectan a la red de telefonía o cuando cambian de celda.
- Extraer los metadatos de cada llamada y otros eventos.

Además, la antena falsa Pi2 es invisible a cualquier red o dispositivo y no requiere conectividad y cooperación de los proveedores celulares. Cuenta con un paquete de análisis de datos que permite ordenar, analizar y visualizar los datos e información obtenida en su uso.

247. Ver anexo B del contrato DAD-ADQ-PGJE-39-15, "Contrato de suministro de equipamientode vigilancia, análisis de comunicaciones y forense celular para la Procuraduría General de Justicia del Estado de Baja California", disponible en: https://r3d.mx/wp-content/uploads/Contrato-IMSI-Catcher-Baja-California.pdf

248. Verint, Tactical Off- Air Intelligence Solutions, *op. cit.*, disponible en: https://r3d.mx/wp-content/uploads/1278-verint-product-list-engage-gi2-engage-pi2.pdf

Gráfico 3.5. Verint - Engage Pi2. Folleto informativo.

d. GAXG de Rohde & Schwart

Otro de los modelos detectados es el desarrollado por la empresa alemana ***Rohde & Schwartz***, que se dedica al desarrollo de una gran gama de productos electrónicos, entre estos, algunos dentro del campo de telecomunicaciones.

En 2017, mediante el contrato FGE/FASP/004/2017,[249] la Fiscalía General de Justicia del Estado de Quintana Roo adquirió a la empresa *Rohde & Schwarz de México , S. de R.L. de C.V.* un equipo de antena de celular falsa modelo "*GAXG*". De acuerdo a la licitación[250] este equipo es capaz de:

» Realizar llamadas silenciosas, o que no se muestran en el dispositivo llamado pero que son utilizadas entre otras cosas para conocer la ubicación del dispositivo.

» Obtener números de identificación IMSI, IMEI, MSISDN, TMSI, números de identificación de las antenas legítimas, así como la composición del vecindario de estas.

» Prender el micrófono para escuchar.

249. Fiscalía General del Estado de Quintana Roo, Contrato de compraventa relativa a la "adquisición de equipamiento para la Fiscalía General del Estado Partida 4 (equipo de comunicaciones y telecomunicaciones)", FGE/FASP/004/2017, disponible en: https://r3d.mx/wp-content/uploads/Contrato-Quintana-Roo-Rhode-de-Schwarts-México.pdf

250. Fiscalía General del Estado de Quintana Roo, Licitación pública internacional No. FGE-LPI-01-2016 relativa a la adquisición de equipamiento para la Fiscalía General del Estado, Partida 4 (equipo de comunicaciones y telecomunicaciones), Partida 5 (software) y Partida 6 (licenciamiento), disponible en: https://r3d.mx/wp-content/uploads/Licitación-Quintana-Roo-Schwartz.pdf

» Intercepción de llamadas y de mensajes SMS en GSM y GPRS.[251]

» Reenvío de llamadas a antenas legítimas.

» Obtener localización geográfica de los dispositivos conectados.

» Escanéo y análisis de redes 2G/3G.

» Bloqueo de comunicaciones.

» Clonación de SIM (para recibir y enviar mensajes SMS y recibir y realizar llamadas como si fuera el dispositivo clonado).

» Detección de teléfonos que cambian periódicamente de tarjeta SIM.

» Manipulación de llamadas y mensajes SMS.

» Descifrar cifrado A5/0, A5/1 y A5/2 (presentes en protocolo GSM).

La detección del uso de las antenas falsas no resulta sencilla. Sin embargo, mediciones realizadas por el *Fake Antenna Project* en la Ciudad de México detectaron anomalías en el ecosistema de bases estaciones de telefonía móvil de la ciudad.[252] Aplicando la metodología desarrollada por investigadores de seguridad de la Universidad de Washington para detectar antenas falsas, el proyecto encontró 21 antenas con irregularidades que podrían tratarse de estos dispositivos de vigilancia.

Entre las irregularidades detectadas, algunas se ubican en las zonas del Zócalo capitalino y el Congreso de la Unión. Dichas zonas albergan algunos de los recintos principales del Poder Ejecutivo federal y local (Palacio Nacional y la oficina principal del gobierno de la Ciudad de México), del Poder Judicial (la Suprema Corte de Justicia), y del Poder Legislativo. Además, ambas zonas son centros importantes en los que ocurren concentraciones y protestas, lo que podría explicar el motivo de la probable presencia de las antenas falsas.

También se detectaron irregularidades en la zona aledaña al Colegio Militar cerca de la Salida a la carretera a Cuernavaca, lo que podría sugerir la utilización de esta tecnología por parte de la Secretaría de la Defensa Nacional. Si bien las irregularidades detectadas por *Fake Antenna Project* no son concluyentes ni permiten conocer qué actores se encuentran detrás de dicho uso, nos acercan a esclarecer el uso de esta tecnología de vigilancia, que suele ocurrir fuera del marco de la ley, sin límites ni controles efectivos.

251. Es un protocolo que fue antecesor de los UMTS, que permitía enviar y recibir paquetes de datos que permiten comunicar mensajes multimedia y tener acceso a Internet. Para más información consultar: https://www.master-magazine.info/termino/5172.php

252. Fake Antenna Detection Project (FADE), México CDMX, disponible en: https://fadeproject.org/?project=mexico-df-es&lang=es

La dificultad para detectar este tipo de vigilancia incentiva que su uso ocurra en contextos de opacidad y falta de supervisión, sobre todo en países como México con un alto grado de impunidad y con altos niveles de corrupción. Las antenas falsas solo pueden ser detectadas en el momento en que están siendo utilizadas, debido a que no dejan ningún rastro posterior a su uso en los dispositivos vulnerados o en la red de telefonía. Aunado a esto, estudios académicos[253] han demostrado que inclusive cuando se encuentran en uso, existen varias complicaciones técnicas que hacen difícil su detección.

A partir de las preocupaciones que existen sobre el amplio abuso de antenas falsas, se han desarrollado varias aplicaciones de teléfonos inteligentes cuyo objetivo es su detección. Sin embargo, dichas aplicaciones son falibles,[254] como lo demuestra un estudio desarrollado por académicos de la Universidad de Oxford y de la Universidad de Berlín.

La falta de controles, supervisión y transparencia en el uso de estas tecnologías de vigilancia, junto con la dificultad en su detección, fomenta el amplio abuso de este tipo de vigilancia por parte de autoridades y de entes privados.[255] Adicionalmente, la naturaleza masiva de la vigilancia que las antenas falsas permiten contradice los principios constitucionales de inviolabilidad de las comunicaciones privadas, las cuales requieren que cualquier injerencia en este derecho se encuentre focalizada a personas en específico y cuente con autorización judicial federal previa.

D. 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** o **SS7** es un conjunto de protocolos que permite el intercambio de información entre empresas de telecomunicaciones y entre componentes de la red de telefonía, con el fin de facilitar la provisión de este servicio.

---

253. Dabroski, A., *et.al.*, "IMSI-Catch Me If You Can: IMSI-Catcher-Catchers", *ACM*, 8 de diciembre de 2014, disponible en: https://dl.acm.org/doi/10.1145/2664243.2664272
También véase: Ney, P. et. al., "SeaGlass: Enabling City-Wide IMSI-Catcher Detection", De Gryuter, 2017, disponible en: https://www.researchgate.net/publication/318305068_SeaGlass_Enabling_City-Wide_IMSI-Catcher_Detection

254. Martin, A. y Shinjo P., "White-Stingray: Evaluating IMSI Catchers Detection Applications", USENIX Association, 2017, disponible en: http://www.cs.ox.ac.uk/files/9192/paper-final-woot-imsi.pdf pg. 10.

255. Cushing, T., "Israeli-Made Stingray Device Found In The Hands Of South African Businessmen", *Techdirt*, 14 de agosto de 2015, disponible en: https://www.techdirt.com/articles/20150811/10003831913/israeli-made-stingray-device-found-hands-south-african-businessmen.shtml

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.

Entre las capacidades de vigilancia que el abuso de este protocolo otorga se encuentran las siguientes:

» Conocer la localización de los dispositivos conectados a la red móvil.

» Conocer el número IMSI, el número IMEI y el estado del dispositivo (ausente, conectado, no disponible, ocupado).

» Interceptar llamadas, mensajes y uso de datos móviles.

» Interferir, bloquear y afectar el funcionamiento y la conectividad de la red de comunicación.

» Realizar llamadas y enviar mensajes fraudulentos personificando números telefónicos u otros entes.

Actualmente, con la expansión y diversificación del sector de telecomunicaciones móviles, el acceso al protocolo puede ser fácilmente comprado y es utilizado de manera ilegítima por actores diferentes a las empresas de telecomunicaciones. Varias empresas como *Verint* y *Rayzone* han desarrollado herramientas de vigilancia que explotan la vulnerabilidad en el SS7. Se ha documentado que varias autoridades en México han comprado y hecho uso ilegal de dichas herramientas de vigilancia, principalmente con fines de geolocalización.

Por ejemplo, ***Rayzone Group*** es un conglomerado israelí que comercializa equipos de intervención de comunicaciones, localización geográfica en tiempo real y análisis de información. Se ha comprobado que la Fiscalía General de la República suscribió, entre 2019 y 2020, al menos cuatro contratos para la adquisición de estas tecnologías de vigilancia.[256] En todas las ocasiones, la Fiscalía utilizó como intermediaria a la empresa *Neolinx de México*, dedicada a la venta de equipo de espionaje durante el gobierno de Enrique Peña Nieto.[257]

256. R3D, "#FiscalíaEspía: la FGR adquirió equipo capaz de espiar ilegalmente a todos los usuarios de Internet en México", 14 de abril de 2021, disponible en: https://r3d.mx/2021/04/14/fiscaliaespia-la-fgr-adquirio-equipo-capaz-de-espiar-ilegalmente-a-todos-los-usuarios-de-internet-en-mexico/

257. Neolinx estuvo involucrada, entre 2014 y 2015, en procesos de venta de sistemas de vigilancia a la SEDENA, al Centro de Investigación y Seguridad Nacional (CISEN), la Policía Federal y la Procuraduría General de la República.

De acuerdo con el Anexo Técnico de uno de los contratos celebrado con la Dirección General de Cuerpo Técnico de Control de la SIEDO en abril de 2018,[258] ***Geomatrix*** puede brindar acceso a 25 operadores simultáneos para teléfonos en redes 2G, 3G y 4G. El sistema permite solicitar la localización geográfica en tiempo real de un equipo proporcionando el número de teléfono o el número IMSI (Identidad Internacional de Suscriptor Móvil). Otra de las características de *Geomatrix* es el uso de geovallas; es decir, se establece un perímetro virtual en el mapa y el sistema indica cuándo un equipo ha ingresado o salido de sus límites.

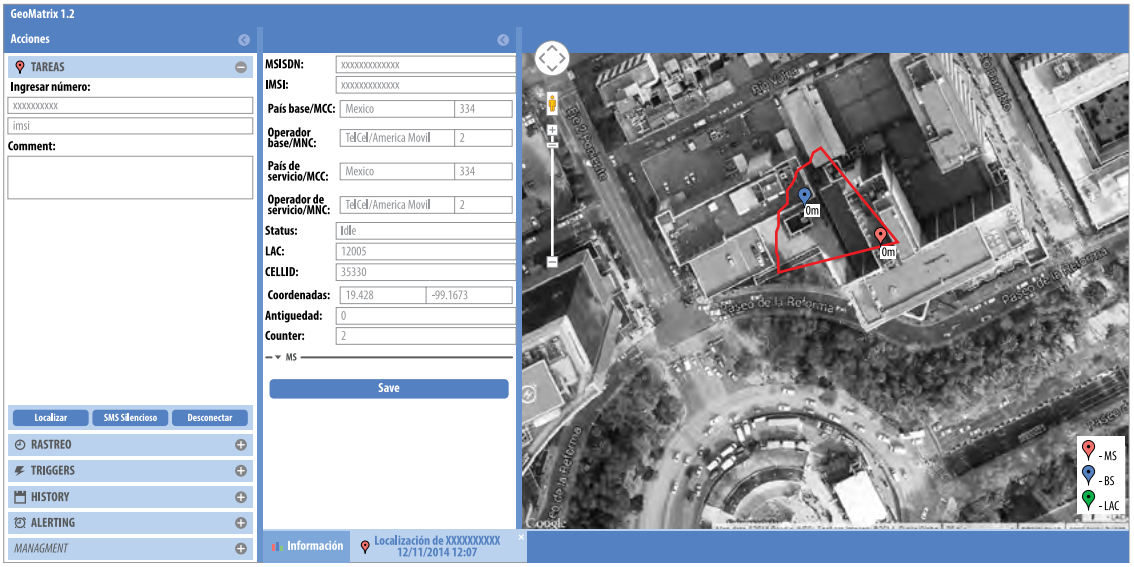


Gráfico 3.6. Parte de la presentación del sistema GeoMatrix, contenida en uno de los correos filtrados de la empresa Hacking Team.[259]

La vigilancia que se ejerce mediante la explotación del protocolo SS7 no requiere que el atacante esté cerca del dispositivo que desea vigilar. Este tipo de tecnología permite vigilar dispositivos en cualquier parte del mundo (en donde haya cobertura de telefonía móvil). El único dato que es necesario conocer es el número telefónico o el número IMSI de los dispositivos de los objetivos.

La conjunción entre el abuso del protocolo SS7 y el uso de una antena falsa (*IMSI Catcher*) permite al atacante obtener acceso y control aún más profundo a los dispositivos vigilados. Por

258. "Contratación para la prestación del servicio de localización geográfica en tiempo real, para equipos de comunicación móvil asociados a una línea telefónica", Anexo Técnico, 2018, disponible en: https://r3d.mx/wp-content/uploads/Anexo-tecnico-Geomatrix-SEIDO.pdf

259. *Geomatix. Positioning of Mobile Phones System.* (PDF) https://wikileaks.org/hackingteam/emails/fileid/45152/20770

ejemplo, mediante el protocolo SS7 es posible obtener las llaves de cifrado con el que cuentan las comunicaciones 3G y 4G y utilizarlo para autenticar las antenas falsas con los dispositivos que se buscan conectar a estas. Con esto, se hace más difícil la detección de una antena falsa, puesto que no es necesario degradar la comunicación a protocolos inferiores al 3G.

Otra posible aplicación del uso conjunto de *IMSI catchers* y de sistemas de vigilancia mediante el protocolo SS7 está relacionada con la identificación de asistentes a eventos masivos, sin la necesidad de contar con el apoyo de empresas de telecomunicaciones. Mediante el uso de una antena falsa es posible obtener números telefónicos, IMEI y conocer la ubicación de los dispositivos. A partir de esta información, mediante el protocolo SS7 es posible solicitar la información de identificación de las suscriptoras y mantener un seguimiento de su ubicación.

Además, el hecho de que los sistemas de vigilancia mediante el protocolo funcionen a través de una intromisión a nivel de la red central de telefonía complica su detección. Varios Estados han implementado medidas enfocadas en limitar vulnerabilidades presentes en el protocolo SS7.[260] Sin embargo, según expertos en telecomunicaciones, la complejidad con la que cuentan las redes de telecomunicaciones provoca que la adopción de estas medidas sea sumamente costosa y que afecte de manera negativa el funcionamiento del sistema.

Una investigación periodística publicada por el diario israelí *Haaretz* reveló una infraestructura de vigilancia global, mantenida por Andreas Fink —un experto en telecomunicaciones suizo y excolaborador de Julian Assange—, que aprovecha las vulnerabilidades del sistema de comunicaciones móviles para permitir que gobiernos y empresas puedan geolocalizar dispositivos.[261] Es importante mencionar que, si bien la compra de herramientas de geolocalización no es necesariamente ilegal, su uso sin las debidas salvaguardas sin autorización judicial lo es.

El reportaje señala que los sistemas de Fink han permitido numerosos ataques a redes telefónicas en todo el mundo, incluyendo en América, y menciona el caso del periodista Fredid Román Román, cuyo teléfono fue geolocalizado un día antes de su asesinato en Chilpancingo, Guerrero, el 22 de agosto de 2022. Román, quien editaba el diario local *La Realidad*, fue acribillado mientras abordaba su vehículo.

En la investigación, Fisk admite que uno de sus clientes actuales es la firma israelí *Rayzone Group*. En México, se han documentado adquisiciones de *Geomatrix* por parte de autoridades

260. GSM Security Map, disponible en: https://gsmmap.org

261. Black, Crofton & Omer Benjakob, "How a Secretive Swiss Dealer Is Enabling Israeli Spy Firms?", *Haaretz*, 14 de mayo de 2023, disponible en: https://www.haaretz.com/israel-news/security-aviation/2023-05-14/ty-article-magazine/.highlight/global-surveillance-the-secretive-swiss-dealer-enabling-israeli-spy-firms/00000188-0005-dc7e-a3fe-22cdf2900000

estatales tales como Baja California, Hidalgo, Jalisco, Puebla, Querétaro, Tabasco, Veracruz y Yucatán; así como la Fiscalía General de la República, que suscribió al menos cuatro contratos entre 2019 y 2020 para hacerse de este servicio.

La siguiente tabla muestra casos en los que autoridades mexicanas han adquirido este tipo de sistemas de vigilancia:

Autoridad	Proveedor	Folio del contrato	Año	Objeto	Marca	Monto de compra (incluye I.V.A.)
Procuraduría General de Justicia del Estado de Baja California	Eyetech Solutions S.A. de C.V.	DAD-ADQ-PGJ E-47-14	2014	200 búsquedas diarías por un año del Sistema LightHouse	EyeTech Solutions	$85.840.000,00 (incluye otros sistemas)
		DAD-ADQ-PGJ E-59-15	2015	200 búsquedas diarías por un año del Sistema LightHouse	EyeTech Solutions	$32.000.000,00 (incluye otros sistemas)
		DAD-ADQ-PGJ E-112-16	2016	200 búsquedas diarías por un año del Sistema LightHouse	EyeTech Solutions	$20.495.310,00
Fiscalía General de Chiapas	NC	NC	2017	Sistema GeoMatrix, 12070 consultas	Rayzone	$14.065.812,00
Fiscalía General de Hidalgo	Neolinx de México, S.A. de C.V.	359/19	2019	Sistema GeoMatrix, 1000 consultas	Rayzone	$ 1,034,300.00
Fiscalía General de Querétaro	Neolinx de México, S.A. de C.V.	NC	2018	1115 consultas, se desconoce el sistema	NC	$1.014.304,00
Fiscalía General de la República	Neolinx de México, S.A. de C.V.	NC	2018	Sistema GeoMatrix, 255 500 consultas	Rayzone	$4.500.000,00 (dólares)
Oficialía Mayor del Estado de San Luís Potosí	Eyetech Solutions S.A. de C.V.	DGA-CAASPE-AD-40-13	2013	Sistema LightHouse 100 búsquedas diarias	EyeTech Solutions	$19.000.000,00
Fiscalía General de Justicia del Estado de Sonora	Neolinx de México, S.A. de C.V.	FGJE/FASP/040 /2014	2014	Sistema GeoMatrix, 1626 consultas	Rayzone	$1.445.605,67
		FGJE/FASP/040 /2014	2014	Sistema GeoMatrix, 1626 consultas	Rayzone	$1.445.605,67
Fiscalía General de Veracruz	Neolinx de México, S.A. de C.V.	AD 18/14	2014	Sistema GeoMatrix, 3285 consultas	Rayzone	$3.200.000,00

Tabla 3.7. Autoridades mexicanas que han adquirido sistemas de geolocalización basada en la explotación de vulnerabilidades del SS7. Solicitudes de acceso a la información.

Adicionalmente el medio digital *Animal Político*[262] ha documentado la adquisición de los siguientes sistemas de geolocalización que explotan vulnerabilidades en el protocolo SS7:

Entidad	Autoridad	Herramienta
Baja California Sur	Secretaría de Seguridad Pública de Baja California Sur	Rayzone – Geomatrix
Ciudad de México	Fiscalía General de Justicia de la Ciudad de México	TGR Dashboard
Durango	Fiscalía General del Estado de Durango	Rayzone – Geomatrix
Estado de México	Fiscalía General de Justicia del Estado de México	TGR Dashboard
Hidalgo	Secretaría de Seguridad Pública de Hidalgo	Rayzone – Geomatrix
Jalisco	Secretaría General de Gobierno	Rayzone – Geomatrix
Jalisco	Fiscalía General del Estado de Jalisco	Rayzone – Geomatrix
Oaxaca	Fiscalía General del Estado de Oaxaca	Rayzone – Geomatrix
Puebla	Fiscalía General del Estado de Puebla	Rayzone – Geomatrix
Tabasco	Comisión de Búsqueda de Personas de Tabasco	Rayzone – Geomatrix

Tabla 3.8. ***Tabla 3.7. Autoridades mexicanas que han adquirido sistemas de geolocalización basada en la explotación de vulnerabilidades del SS7. Animal Político.***

Según investigaciones del diario *El País*,[263] el medio *Reporte Índigo* y R3D, existe evidencia de que la Fiscalía General de la República ha adquirido y operado ilegalmente el sistema

262. Valencia, René & Karla Cejudo, "Sedena y 37 instituciones estatales intervinieron celulares y computadoras en el actual sexenio sin lograr ni una detención", *Animal Político*, 10 de julio de 2024, disponible en: https://animalpolitico.com/seguridad/ejercito-compra-tecnologia-vigilar-celulares-computadoras

263. Gallegos, Zorayda, "La Fiscalía de México ha contratado en los dos últimos años programas para el espionaje masivo de teléfonos móviles", *El País*, 14 de abril de 2021, disponible en: https://elpais.com/mexico/2021-04-14/la-fiscalia-de-mexico-ha-contratado-en-los-dos-ultimos-anos-programas-para-el-espionaje-masivo-de-telefonos-moviles.html

de geolocalización para espiar las campañas de los candidatos presidenciales en 2018.[264] Por ejemplo, la investigación de *Reporte Índigo* apunta que se celebraron las campañas electorales de 2018 (30 de marzo de 2018) dos días antes de que se firmara y reservara la información del contrato por cinco años, periodo en donde además se dio el número más elevado de geolocalizaciones.[265]

La investigación de *Reporte índigo* documentó que la Fiscalía adquirió la capacidad para hacer 255 mil búsquedas, sin límite diario, de marzo de 2018 a marzo de 2019. En dicho periodo, la FGR solo pidió autorización judicial para ejercer 101 solicitudes de localización geográfica.

Además, al contrastar la información con lo documentado por la Auditoría Superior de la Federación[266] se comprueba el uso ilegal del equipo. Según la ASF, al menos uno de los contratos celebrados por la Fiscalía se formalizó sin autorización de recursos previa ni especificar el costo unitario de cada concepto del servicio. Tampoco se encontró evidencia que acreditara la configuración del servicio en los equipos de la Fiscalía, aunado a que la ASF señaló en su informe que "*no se proporcionó evidencia de los certificados o constancias otorgados a 39 servidores públicos*" respecto de la capacitación para utilizar *Geomatrix*.

A pesar de que la FGR contrató 135 mil búsquedas, la ASF comprobó el ejercicio de 13,890 (10.3%). Esta información fue contrasta con la reportada por la propia Fiscalía en la Plataforma Nacional de Transparencia, donde indica haber solicitado autorización judicial para la localización geográfica únicamente 124 veces durante 2019. Lo anterior indica que al menos en el 99.1 por ciento de las ocasiones, el equipo se utilizó de forma ilegal.

E. *Outsourcing* de la vigilancia masiva

Una novedosa herramienta de vigilancia masiva recientemente detectada en México ha consistido en el ***outsourcing* de la vigilancia a empresas privadas**. En este caso, empresas privadas vigilan masivamente a la población mediante la adquisición y agregación de múltiples bases de datos –principalmente datos de localización–, algunas adquiridas a través del opaco mercado de aplicaciones y servicios de internet con fines de publicidad digital y otras de procedencia desconocida, e incluso, de origen legalmente cuestionable.

264. R3D, "#FiscalíaEspía: La FRG adquirió equipo capaz de espiar ilegalmente a todos los usuarios de internet en México", 14 de abril de 2021, disponible en: https://r3d.mx/2021/04/14/fiscaliaespia-la-fgr-adquirio-equipo-capaz-de-espiar-ilegalmente-a-todos-los-usuarios-de-internet-en-mexico/

265. Reporte índigo, "Espionaje sin controles", 5 de junio de 2019, disponible en: https://www.reporteindigo.com/reporte/espionaje-sin-controles-pgr-adquisicion-doftware-geolocalizacion-periodo-electoral/

266. Respecto del contrato FGR/SEIDO/DGCTC/GSPN/001/2019, en su auditoría a la partida presupuestaria 33701 de la FGR, correspondiente a Gastos de Seguridad Pública y Nacional.

Estas empresas privadas desarrollan herramientas y ofrecen a sus clientes la posibilidad de realizar búsquedas a partir de datos como un correo electrónico, número de teléfono u otros identificadores. Si una cuenta de una aplicación o servicio en Internet se encuentra asociada a esos identificadores y la empresa de vigilancia adquirió dicha base de datos de localización, el servicio otorga la ubicación, fecha, hora y otros datos en las que se detectó actividad en dicha aplicación o servicio.

Uno de los ejemplos de este *outsourcing* de la vigilancia es la plataforma ***Echo***, un sistema de consulta y análisis de datos masivos, desarrollada por ***Echo-On Technologies***, empresa subsidiaria del anteriormente mencionado *Rayzone Group*. El sistema proporciona a las autoridades información diversa sobre personas usuarias de Internet, de manera incógnita, sin requerir la colaboración del individuo u otra entidad comercial.

Según la propia descripción del producto en su sitio web, *Echo* funciona independientemente del tipo de dispositivo o sistema operativo, no requiere de instalación y puede obtener información de un individuo en específico y hacer incluso "*recopilación en masa de todos los usuarios de Internet en un país*".[267]

Reportes periodísticos han indicado que *Echo* funciona mediante el acceso a datos de localización recolectados por diferentes plataformas de publicidad móvil.[268] Sin embargo, la empresa no ha dejado en claro de qué forma consigue acceder a esa información. De este modo, la plataforma es capaz de proporcionar la geolocalización de un dispositivo con un margen de error de un metro y con un ligero desfase respecto al tiempo real.

267. ECHO – Sistema Virtual Global Sigint, disponible en: https://web.archive.org/web/20211018201403/https://rayzone.com/es/echo-sistema-virtual-global-sigint/

268. Ganon, Tomer & Hagar Ravet, "The Rayzone Group's secret cyber intelligence activities revealed", *Calcalistech*, 29 de diciembre de 2020, disponible en: https://www.calcalistech.com/ctech/articles/0,7340,L-3884553,00.html

Gráfico 3.7. Sistema Virtual Global Sigint. Sitio web de Rayzone.

Según información publicada por el diario *El País* e informes de la Auditoría Superior de la Federación, la Fiscalía General de la República (FGR) adquirió este servicio en los años 2019 y 2020 por montos de 1.1 y 1.7 millones de dólares, respectivamente.[269] Nuevamente, la operación fue realizada a través de la empresa *Neolinx de México S.A. de C.V.*, quién también fue la intermediaria para la adquisición de *Geomatrix*, otro de los productos de *Rayzone Group*.

De acuerdo con un informe de auditoría del Órgano Interno de Control de la FGR,[270] fechada en agosto de 2020, el contrato FGR/CMI/AIC/PFM/CN/GSN/SERV/001/2019 estuvo vigente del 1 de septiembre al 31 de diciembre de 2019, mientras que en el contrato FGR/CMI/AIC/PFM/CN/GSN/SERV/001/2020 se informa que el servicio fue proporcionado del 1 de enero al 31 de mayo de 2020.

269. Gallegos, Zorayda, "La Fiscalía de México ha contratado en los dos últimos años programas para el espionaje masivo de teléfonos móviles", *op. cit.*, disponible en: https://elpais.com/mexico/2021-04-14/la-fiscalia-de-mexico-ha-contratado-en-los-dos-ultimos-anos-programas-para-el-espionaje-masivo-de-telefonos-moviles.html

270. Órgano Interno de Control de la Fiscalía de la República, Área de Auditoría Interna, Auditoría 8/2020 "Compras y Gastos en Seguridad Pública y Nacional", UR Auditada: Policía Federal Ministerial, Del primero de enero de 2019 al 31 de mayo de 2020, disponible en: https://r3d.mx/wp-content/uploads/OIC_Auditoria_08-2020_Observaciones.pdf

CAPÍTULO CUATRO

Diagnóstico de la vigilancia en México

A partir del análisis de la regulación y la práctica de la vigilancia de comunicaciones en México, contrastada con los estándares internacionales en materia de protección de derechos humanos aplicables a esta actividad, se presenta el siguiente diagnóstico que resume las deficiencias, desafíos y problemas que requieren ser corregidos para revertir la impunidad con que la vigilancia de comunicaciones es abusada en México.

I. Incertidumbre jurídica

Como fue advertido en el Capítulo Segundo del Informe, la regulación de la vigilancia de comunicaciones posee diversas deficiencias que producen incertidumbre jurídica.

A. Sobre las autoridades facultadas

A pesar de que la Constitución, las leyes y la interpretación de la SCJN[271] únicamente reconocen como autoridades facultadas expresamente para llevar a cabo medidas de vigilancia de comunicaciones a la Guardia Nacional (GN), el Centro Nacional de Inteligencia (CNI), la Fiscalía General de la República (FGR), las 32 fiscalías estatales y la Fiscalía General de Justicia Militar (FGJM), en el marco de sus respectivas competencias, persisten autoridades federales y locales que derivan facultades para vigilancia de comunicaciones, como la geolocalización en tiempo real o el acceso a datos conservados por empresas de telecomunicaciones, de normas vagas e imprecisas o las llevan a cabo sin fundamentación alguna.

Esta incertidumbre jurídica no solamente aumenta los riesgos para las personas potencialmente vigiladas ilegalmente en perjuicio de su privacidad y seguridad, sino que puede con-

271. Ver por ejemplo: **Amparo en Revisión 964/2015**. Sentencia de 4 de mayo de 2016, resuelta por unanimidad de cinco votos de los señores Ministros: Eduardo Medina Mora I., Javier Laynez Potisek, José Fernando Franco González Salas, Margarita Beatriz Luna Ramos y Presidente Alberto Pérez Dayán (ponente). Los señores Ministros José Fernando Franco González Salas y Margarita Beatriz Luna Ramos emitieron su voto en contra de consideraciones, pp. 63 a 64.

llevar responsabilidad legal para las empresas que colaboran en el despliegue de las medidas de vigilancia, e incluso puede poner en riesgo la validez jurídica de actuaciones por parte de autoridades, lo cual puede ocasionar perjuicios al interés público.

B. Sobre los requisitos de procedencia material

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, a pesar de que la Ley de la Guardia Nacional (en adelante, LGN) requiere que se constate "*la existencia de indicios suficientes que acrediten que se está organizando la comisión de delitos*" enlistados en el artículo 103 de la LGN, otros ordenamientos poseen requisitos de procedencia amplios y vagos. Resalta la Ley de Seguridad Nacional (en adelante, LSN), la cual permite medidas como la intervención de comunicaciones cuando a juicio del CNI existan "*amenazas a la seguridad nacional*", las cuales son definidas de manera amplia y vaga en el artículo 5 de la LSN.

Igualmente, en algunos casos, el Código Nacional de Procedimientos Penales (en adelante, CNPP) faculta a las fiscalías a llevar a cabo medidas de vigilancia cuando el propio Ministerio Público las considere necesarias. 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 defiere en exceso a la propia autoridad para justificar la pertinencia de una medida de vigilancia.

C. Sobre el control judicial previo o inmediato

Reformas al CNPP y algunos precedentes judiciales han establecido con mayor claridad la necesidad de control judicial previo, como regla general, para llevar a cabo medidas de vigilancia como el acceso a datos conservados por empresas de telecomunicaciones o la geolocalización en tiempo real. Sin embargo, persiste la incertidumbre jurídica respecto del control judicial de las medidas de vigilancia.

Por ejemplo, el mecanismo excepcional establecido en el artículo 303 del CNPP faculta que las fiscalías pueden 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–, pernitiendo 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.

Por otro lado, si bien precedentes recientes de la SCJN han establecido con claridad que la autoridad judicial federal es la autoridad judicial competente para evaluar las solicitudes de autorización para la intervención de comunicaciones privadas, el acceso a datos conservados o la geolocalización en tiempo real,[272] varias autoridades persisten en pretender que las autoridades judiciales locales puedan tener competencia para autorizar dichas medidas de vigilancia.

Peor aún, diversas autoridades parecen interpretar que el requisito de autorización judicial previa resulta únicamente aplicable a medidas de vigilancia que requieren la colaboración de terceros, como empresas de telecomunicaciones o proveedores de servicios, aplicaciones y contenidos en Internet, y no así cuando las autoridades despliegan medidas de vigilancia de manera autónoma, por ejemplo, a través de tecnologías de geolocalización como aquellas que explotan las vulnerabilidades en el protocolo SS7; o incluso medidas de vigilancia masiva como las antenas falsas o la vigilancia masiva delegada a particulares con herramientas como *Echo*.

La elusión del control judicial a las medidas de vigilancia fomenta los abusos, impiden la detección de los mismos y permiten la impunidad que fomenta su repetición crónica. Por ello resulta necesario que el marco jurídico detalle con claridad la necesidad del control judicial federal previo o inmediato de todas las medidas de vigilancia reconocidas por el marco jurídico mexicano.

D. Sobre las formas de vigilancia

La proliferación de tecnologías de vigilancia masiva, como las antenas falsas o el *outsourcing* de vigilancia masiva, así como las tecnologías de vigilancia focalizada altamente invasiva y elusiva como el *spyware*, es indicativo de la poca claridad y precisión sobre las métodos de vigilancia que pueden considerarse compatibles con las normas de derechos humanos reconocidas en la Constitución.

Las normas que regulan la vigilancia en el marco jurídico mexicano fueron diseñadas pensando en tecnologías de intervención telefónica y otras formas de vigilancia focalizada que requerían la colaboración de particulares, especialmente empresas de telecomunicaciones. Los métodos tradicionales de vigilancia de comunicaciones ofrecían considerablemente menos información de las personas vigiladas y producían ineludiblemente testigos en las empresas de telecomunicaciones que colaboraban con dicha vigilancia, las cuales –en teoría– podrían resultar menos propensas a colaborar con intervenciones ilegales, es decir, aquellas no autorizadas por un juez competente.

272. Plenos Regionales. Tesis PR.P.CN. J/23 P (11a.) Gaceta del Semanario Judicial de la Federación. Libro 33, Enero de 2024, Tomo IV, página 3989. Registro digital: 2028011; y SCJN. Primera Sala. Tesis 1a. VI/2024 (11a.) Gaceta del Semanario Judicial de la Federación. Libro 37, Mayo de 2024, Tomo II, página 2250. Registro digital: 2028870.

Sin embargo, tecnologías de *spyware* como *Pegasus* ofrecen una cantidad de información que no se limita a las conversaciones telefóncias de la persona vigilada, sino que permiten el acceso a información como contactos, fotografías, videos, archivos, mensajes de texto, geolocalización, contraseñas, historial de navegación, entre otra información que permite dibujar un panorama más completo de la vida privada de la persona vigilada, lo cual constituye una invasión intensa y sin paralelo a la intercepción telefónica tradicional.

Además, el hecho de que para ser desplegadas, dichas tecnologías no requieren la colaboración de terceros, sino que son utilizadas de manera autónoma por la autoridad atacante, añadido a las características antiforenses y antidetección, implica un enorme desafío para evitar su utilización ilegal. Resulta poco sensato pretender que el marco jurídico actual es capaz de asegurar su utilización racional o incluso la posibilidad de que dichas tecnologías puedan siquiera ser compatibles con los principios de necesidad y proporcionalidad.

Igualmente, además de que del marco constitucional y convencional se desprende la necesidad de que las medidas de vigilancia de comunicaciones se encuentren focalizadas a personas específicas, la proliferación y uso cotidiano de tecnologías de vigilancia masiva indican que el marco jurídico actual no ha ofrecido claridad suficiente para inhibir la adquisición y uso de dichas tecnologías de vigilancia.

II. Irregularidades y corrupción en la adquisición de tecnologías de vigilancia

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.

Dentro de las principales irregularidades respecto de los procesos de contratación de equipos y sistemas para la vigilancia destacan las siguientes:

A. Discrecionalidad y adjudicación a empresas con irregularidades

Prácticamente la totalidad de las contrataciones relacionadas a equipos o sistemas para la vigilancia de comunicaciones que han sido documentadas se han realizado mediante adjudicación directa, lo cual fomenta la discrecionalidad en la selección de empresas contratadas y la opacidad de las mismas.

Derivado de la opacidad y discrecionalidad con la que frecuentemente se han llevado a cabo los procesos de contratación relacionados a equipos y sistemas de vigilancia, así como de la inexistencia de regulación y el establecimiento de requisitos para el ofrecimiento de este tipo de herramientas, se han detectado procesos de contratación en los que la empresa contratada no posee antecedentes o experiencia en la materia o incluso posee irregularidades en su constitución o domicilio legal.

Es el caso de la empresa *Grupo Tech Bull*, la cual contrató con la PGR la venta de equipo y licencias para la operación del sistema *Pegasus* desarrollado por la empresa israelí *NSO Group*. Como ha sido documentado, dicha empresa no poseía antecedentes o experiencia en la materia y no resulta conocida alguna contratación posterior. Además, el socio y administrador único de la empresa desconocía dicha contratación, y las operaciones de la empresa y el domicilio legal de la misma no albergaba oficinas o trabajadores de la misma.

Resulta adicionalmente irregular que los procesos de renovación de dicho contrato con *Grupo Tech Bull* no fueron llevados a cabo con dicha empresa, sino que fueron realizados con las empresas *Proyectos y Diseños VME S.A. de C.V.* para el año 2016 y *Air Cap S.A. de C.V.* para el año 2017.

En diversas jurisdicciones es necesaria una autorización o licencia para la comercialización de equipos o sistemas para tareas de intervención de comunicaciones privadas de manera similar a requisitos para la comercialización de armamento. Sin embargo, en México no existe regulación que exija requisito alguno para ofrecer productos y servicios de esta naturaleza, ni ningún otro tipo de control sobre las empresas que comercializan equipos y sistemas de vigilancia.

B. Sobreprecios en la adquisición de equipos y sistemas de vigilancia

Como consecuencia de las condiciones de discrecionalidad y opacidad, con frecuencia los montos y condiciones de contratación de equipos y sistemas de vigilancia son exorbitantes e irrazonables.

Por ejemplo, en el contrato entre la Dirección General de Cuerpo Técnico de Control de la Subprocuraduría Especializada en Investigación de Delincuencia Organizada (SEIDO) y la empresa *Neolinx de México S.A. de C.V.* para "*la Prestación del Servicio de Localización Geográfica en Tiempo Real, para Equipos de Comunicación Móvil Asociados a una Línea Telefónica*", se adquirió la capacidad de 255 mil 500 búsquedas de monitoreo de la localización geográfica de equipos de comunicación móvil dentro de un plazo de 9 meses (de abril a diciembre de 2018).[273]

273. SEIDO. Anexo Técnico de la Contratación para la prestación del servicio de localización geográfica en tiempo real, para equipos de comunicación móvil asociados a una línea telefónica. Disponible en: https://r3d.mx/wp-content/uploads/Anexo-tecnico-Geomatrix-SEIDO.pdf

Según datos reportados por la PGR a la Plataforma Nacional de Transparencia (PNT), durante el año 2018, dicha dependencia únicamente realizó 207 solicitudes de localización geográfica en tiempo real. Igualmente, según datos del Poder Judicial de la Federación (PJF),[274] en 2018, recibió un total de 27,849 solicitudes de autorización judicial para intervención de comunicaciones privadas, geolocalización en tiempo real y acceso a datos conservados por concesionarias de telecomunicaciones por parte de todas las autoridades facultadas por la ley (no únicamente la PGR).

De lo anterior se desprende un amplio diferencial que solamente puede ser explicado de dos maneras: la utilización masivamente ilegal del sistema de localización geográfica contratado o la enorme subutilización del sistema y consecuente despilfarro de recursos públicos.

Es el mismo caso del sistema *Pegasus*, el cual fue contratado en 2014, con dos renovaciones para los años 2016 y 2017 por montos que oscilan los 40 millones de dólares totales; sin embargo, como la PGR afirmó en el proceso de verificación identificado con la clave INAI.3S.07.01-007/2018, dicha dependencia "*no lo utilizó*".[275] De nuevo, se contempla la posibilidad de una subutilización y el consecuente dispendio injustificado de recursos públicos o, en su caso, la utilización ilegal no reportada del sistema, aunada a la falsedad de declaraciones ante el INAI. Al respecto, la Unidad de Inteligencia Financiera (UIF) de la Secretaría de Hacienda y Crédito Público ha afirmado públicamente haber detectado la adquisición de licencias de *Pegasus* con sobreprecio.[276]

C. Ocultamiento y ofuscación de contrataciones

Frecuentemente, las contrataciones de equipos y sistemas de vigilancia pretenden ser escondidas u ofuscadas a partir de descripciones vagas del objeto de las contrataciones.

Por ejemplo, en el contrato realizado por la Procuraduría General de la República (PGR) para la adquisición de licencias del *spyware Pegasus*, dicho sistema fue denominado "*sistema para la realización de actividades sustantivas*", mientras que la SEDENA lo ha denominado "*Sistema de Monitoreo Remoto de Información*".

274. Presidente de la Suprema Corte de Justicia de la Nación y del Consejo de la Judicatura Federal. Informe Anual de Labores. Disponible en: https://www.cjf.gob.mx/resources/InformeAnual/2018/Informe_Anual_Labores_2018.pdf

275. Versión estenográfica de la sesión ordinaria del Pleno del INAI del día 20 de Febrero de 2019 en donde se resolvió el proceso de verificación identificado con la clave INAI.3S.07.01-007/2018. Páginas 25-26, 35-36.

276. Zerega, Georgina, "El Gobierno de López Obrador asegura que hubo fraude en la compra del 'software' espía Pegasus", *El País*, 16 de febrero de 2024, disponible en: https://elpais.com/mexico/2024-02-16/el-gobierno-de-lopez-obrador-asegura-que-hubo-fraude-en-la-compra-del-software-espia-pegasus.html

De igual manera, en contratos para la adquisición de antenas falsas para la intervención de comunicaciones se han utilizado denominaciones como "*adquisición de equipo activo GSM, para identificación y monitoreo*" o "*fortalecimiento de capacidades para la prevención y combate a delitos de alto impacto*". De manera similar, contratos relacionados a sistemas de análisis forense de dispositivos, como "*Cellebrite*", han sido objeto de contratos denominados "*mobiliario y equipo especializado para chequeo diagnóstico y demás*".

Así mismo, la gran mayoría de contratos relacionados con tareas de vigilancia detectados vía solicitudes de acceso a la información pública o investigaciones periodísticas no aparecen en Compranet, lo que hace aún más difícil identificarlos[277] y detectar irregularidades. De igual manera, aquellas contrataciones que sí aparecen en Compranet frecuentemente no contienen anexos, lo cual impide el acceso efectivo a detalles.[278]

De esta manera, se dificulta la identificación de procesos de contratación relacionados a la adquisición de herramientas y sistemas utilizados en la vigilancia de comunicaciones, lo cual evita la detección de irregularidades por parte de organizaciones periodísticas y de defensa de derechos humanos, e incluso, dificulta el ejercicio de facultades de investigación, por ejemplo, en procesos de verificación llevados a cabo por el INAI o en las carpetas de investigación abiertas por las fiscalías.

Aunado a lo anterior, se ha documentado cómo las autoridades mienten con frecuencia para ocultar contrataciones relacionadas a la viglancia de comunicaciones. Un caso emblemático es el de la SEDENA, respecto del cual se ha documentado que ha mentido en múltiples respuestas a solicitudes de acceso a la información, en las que ha afirmado falsamente no haber celebrado contrataciones con *Comercializadora Antsua S.A. de C.V.* –designada por *NSO Group* como distribuidora exclusiva de *Pegasus*– a pesar de que en documentos enviados a la Auditoría Superior de la Federación y otros documentos internos filtrados se reconoce y evidencia dicha contratación.

D. Ausencia de controles para evitar la adquisición ilegal de tecnologías de vigilancia

A partir de que en México los procesos de adquisición de equipos y sistemas para la vigilancia de comunicaciones no requieren un procedimiento o autorización especial y suelen única-

277. Ver por ejemplo: SSP/PF/CNS/026/2012 - Secretaría de Seguridad Pública - NUNVAV INC - 08/06/2012. Prestación del Servicio de Mantenimiento del Sistema Laguna para la Operación, Análisis y Monitoreo de localización de sistemas de telecomunicaciones y radiocomunicaciones, que operan en el espectro radioeléctrico mexicano.

278. Ver por ejemplo: Expediente 355213 - REQ. 5415 SERVICIO DE INFORMATICA - SEMAR; Expediente 355202 - REQ. 5414 SERVICIOS DE INFORMATICA - SEMAR; Expediente 580008 - REQ. 0402 BIENES INFORMATICOS - SEMAR; y Expediente 1851475 - ADQUISICIÓN DE REFACCIONES PARA EQUIPOS DE RADIOCOMUNICACIÓN TÁCTICA EN HF - SEDENA.

mente involucrar a la autoridad y empresas contratantes, sin la intervención de ninguna otra dependencia, se ha fomentado la realización de contrataciones por parte de autoridades sin facultades de vigilancia de comunicaciones.

Como muestra, se ha reportado la adquisición del malware *Pegasus* por parte de la SEDENA y su utlización por parte del Centro Militar de Inteligencia, a pesar de que la dependencia no cuenta con facultades para operar dicha herramienta para tareas de inteligencia. De igual manera, se ha documentado la adquisición de licencias para el uso de malware de vigilancia comercializado por la empresa italiana *Hacking Team* por parte de múltiples autoridades sin facultades, por ejemplo, la Secretaría de Gobierno del Estado de Jalisco, la Secretaría de Planeación y Finanzas del Gobierno de Baja California o incluso Petróleos Mexicanos.[279]

Adicionalmente, a pesar de que la Constitución, los tratados internacionales de derechos humanos y las leyes imponen límites a las autoridades respecto de las injerencias en la vida privada que resultan admisibles, no existe ningún mecanismo capaz de detectar y evitar que sean adquiridos equipos y sistemas que excedan esos límites o faciliten la elusión de mecanismos de rendición de cuentas.

Por ejemplo, a pesar de que la intervención de comunicaciones privadas únicamente es admisible cuando exista una autorización judicial federal que justifique la utilización de dicha medida de manera focalizada, se ha documentado la adquisición de herramientas y sistemas que permiten injerencias en la vida privada y las comunicaciones privadas de manera masiva, es decir, respecto de un número amplio o indeterminado de personas. Es el caso de las antenas falsas, también conocidas como *IMSI catchers*, en cuya operación interfieren con un número indeterminado de personas que se encuentran en la proximidad de dichas antenas, por lo que la legalidad de su operación es altamente cuestionable, y en el mismo sentido, su adquisición.

Igualmente, resulta problemática la adquisición de sistemas diseñados para eludir la rendición de cuentas, es decir, sistemas que no dejan rastros o registros de su operación, dificultando procesos de investigación futuros sobre denuncias de abuso de dichos sistemas, como es el caso del malware *Pegasus*.

Existen experiencias de regulación que exigen la obtención de autorizaciones y el registro de adquisiciones o exportaciones respecto de bienes como armas, municiones, vehículos o "*tecnologías de doble uso*", dentro de las cuales en ocasiones se ubican equipos y sistemas de vigilancia. Por ejemplo, en el artículo 124 de la Ley General del Sistema Nacional de Seguridad Pública se contempla el Registro Nacional de Armamento y Equipo, en el que se incluyen

279. R3D. *El Estado de la Vigilancia*. Noviembre de 2016. Página 83. Disponible en: https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016.pdf

vehículos y armamento. De manera similar, el Reglamento Europeo "*por el que se establece un régimen comunitario de control de las exportaciones, la transferencia, el corretaje y el tránsito de productos de doble uso*" establece diversos procesos de autorización y registro respecto de bienes dentro de los cuales se ubican algunas tecnologías para la intervención de comunicaciones privadas.[280]

Así mismo, es importante resaltar que las contrataciones públicas son un instrumento importante para la promoción de derechos humanos en México y en el mundo.[281] De manera similar a como algunas legislaciones en el mundo establecen, México tiene la responsabilidad de asegurar que a través de las contrataciones públicas no está beneficiando a empresas involucradas en la violación de derechos humanos en cualquier parte del mundo.

Finalmente, la adquisición de este tipo de tecnologías desarrolladas en en el extranjero puede conllevar riesgos en materia de seguridad nacional respecto de los cuales no existe un proceso capaz de evaluar o remediar de manera previa o posterior a la adquisición y despliegue.

III. Ausencia de documentación sobre la adquisición y uso de equipos y sistemas de vigilancia

Aún cuando, como se ha afirmado, la legislación es deficiente en establecer procedimientos especializados para la adquisición y uso de equipos y sistemas de vigilancia, las autoridades suelen incumplir hasta los más mínimos requisitos de documentación.

Con frecuencia, las autoridades han afirmado no contar con información básica de los procesos de contratación, como estudios de mercado, opiniones de las áreas correspondientes o registros de cadena de custodia de los equipos. Al grado que en algunas ocasiones, no ha sido posible verificar la ubicación material de los equipos y sistemas.

Adicionalmente, a pesar de que el marco jurídico exige la existencia de registros sobre las medidas de vigilancia de comunicaciones, con frecuencia las autoridades alegan la inexistencia de dichos registros.

---

280. Reglamento (CE) no 428/2009 del Consejo de 5 de mayo de 2009 por el que se establece un régimen comunitario de control de las exportaciones, la transferencia, el corretaje y el tránsito de productos de doble uso.

281. Ver, por ejemplo la Sección 1502 de la "Dodd-Frank Wall Street Reform and Consumer Protection Act' de los Estados Unidos sobre la utilización de minerales en conflicto o el artículo 8 del Reglamento (CE) no 428/2009 del Consejo de 5 de mayo de 2009 por el que se establece un régimen comunitario de control de las exportaciones, la transferencia, el corretaje y el tránsito de productos de doble uso.

Esta ausencia de documentación fomenta el abuso, obstaculiza la transparencia y el ejercicio de las facultades de supervisión e investigación que poseen diversas autoridades, lo cual también favorece la impunidad.

IV. Vigilancia ilegal

Además de la adquisición y uso de equipos y sistemas de vigilancia de comunicaciones por parte de autoridades sin facultades legales, existe amplia evidencia del abuso de dichas herramientas.

A. Espionaje a personas periodistas, defensoras de derechos humanos, activistas y opositoras políticas

Como ha sido establecido con detalle en el Capítulo Tres de este informe, 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.

Por ejemplo, está ampliamente documentado el uso de *spyware* como *Galileo* de la empresa italiana *Hacking Team* en contra de periodistas y políticos en estados como Puebla o Baja California; un caso en donde inclusive personas admitieron culpabilidad ante el sistema judicial de Estados Unidos por comercializar y utilizar *spyware* ilegalmente y a sabiendas de su uso ilegal.

Se destaca la amplia evidencia de abuso del *spyware Pegasus*, desde su adquisición y operación ilegal por parte de las áreas de inteligencia del Ejército mexicano, así como su utilización en contra de periodistas, personas defensoras de derechos humanos y activistas, como ya ha sido detallado en este Informe.

También se destaca la evidencia de acceso ilegal a datos conservados por empresas de telecomunicaciones, así como el uso de tecnologías de vigilancia masiva respecto de periodistas, personas defensoras de derechos humanos, peritas independientes, funcionarios judiciales y opositores políticos.

La vigilancia de comunicaciones implica una grave interferencia en la vida privada de la persona vigilada, la cual ineludiblemente conlleva afectaciones a las personas con quienes se comunica, incluyendo sus familiares cercanos y sus relaciones profesionales, lo que adquiere una dimensión de gravedad aún mayor respecto de ciertas funciones profesionales.

Por ejemplo, la vigilancia a periodistas compromete a sus fuentes, poniendo en riesgo la revelación de su identidad e incluso su seguridad física. La vigilancia de personas defensoras de derechos humanos compromete la secrecía de las comunicaciones de personas abogadas

con defensores y compromete información de víctimas de violaciones a derechos humanos. As mismo, la vigilancia de personas que ejercen una función pública puede comprometer el ejercicio de sus funciones, haciéndoles vulnerables a la extorsión y el chantaje y, con ello, modificar sus decisiones en perjuicio del interés público y en beneficio de la persona o entidad que ejerce o se beneficia de la vigilancia.

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.

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. Tal es el caso de los periodistas asesinados Fredid Román Román y Cecilio Pineda Brito, respecto de los cuales –como se ha mencionado previamente– existen indicios de haber sido vigilados en momentos previos a su muerte.

B. Acceso ilegal a datos conservados por empresas de telecomunicaciones

Como ha sido documentado, existen graves irregularidades en el sistema de acceso a datos de las comunicaciones de las personas usuarias de telecomunicaciones conservadas por las empresas que prestan dichos servicios.

Por un lado, existen serias discrepancias entre el número de accesos reportados por las autoridades facultadas, el Poder Judicial federal y las empresas de telecomunicaciones, lo que sugiere una práctica generalizada de acceso ilegal a estos datos. Como ejemplo, se encuentra el caso del acceso ilegal a los datos de la periodista Marcela Turati; la cofundadora del Equipo Argentino de Antropología Forense (EAAF), Mercedes Doretti, y la defensora de derechos humanos Ana Lorena Delgadillo.[282]

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.

282. R3D. "SEIDO accedió a registros telefónicos para espiar a periodista y defensoras por investigar masacre de San Fernando", 26 de noviembre de 2021, 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/

Como fue previamente detallado, se ha apreciado un *modus operandi* en el que las fiscalías e 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 al no encontrar utilidad en la información, no resultaba necesario solicitar la ratificación judicial, por lo que, supuestamente se procedió a su destrucción, sin que ello pueda ser verificado.

C. Geolocalización ilegal

Además de que las irregularidades detectadas en los esquemas de acceso a datos conservados por empresas de telecomunicaciones son aplicables a la geolocalización en tiempo real, existe evidencia de geolocalizaciones ilegales llevadas a cabo de manera autónoma por múltiples autoridades en México.

Destaca la proliferación de sistemas de geolocalización que explotan vulnerabilidades en el protocolo SS7 como *Geomatrix* de la empresa *Rayzone Group* y otras herramientas similares, las cuales han sido adquiridas por más de veinte autoridades, muchas de ellas sin facultades legales para llevar a cabo la geolocalización y utilizadas de manera discrecional y clandestina, sin ningún tipo de control judicial previo o inmediato. Destaca el caso de la Fiscalía General de la República, respecto de la cual se encuentra documentada por la Auditoría Superior de la Federación la adquisición y uso irregular del sistema *Geomatrix*.

Con frecuencia se subestima la sensibilidad de los datos de localización, sin embargo, como ya ha sido explicado, los datos de localización permiten derivar el conocimiento de hábitos de movimiento de los que pueden desprenderse aspectos íntimos de la vida de una persona.

La vigilancia de una persona por medio de la geolocalización de su dispositivo móvil, permite identificar fuentes periodísticas, relaciones personales y patrones de movimiento capaces de frustrar actividades de interés público, realizar ataques reputacionales, facilitar la extorsión, e incluso, potenciar amenazas a la seguridad física y la vida de las personas.

Ejemplo de lo anterior, resulta el asesinato del periodista Fredid Román Román cuyo teléfono fue geolocalizado un día antes de su asesinato en Chilpancingo, Guerrero, el 22 de agosto de 2022.

D. Empleo 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.

Lo anterior implica que, por constituir una afectación indiscriminada de los derechos de una cantidad indeterminada de personas, la vigilancia masiva no puede, en ningún caso, considerarse una medida legítima por parte del Estado, sino que la vigilancia debe ser focalizada y justificada por las circunstancias específicas de un caso concreto.

Sin embargo, se ha documentado la adquisición y operación ilegal de herramientas de vigilancia masiva, como lo son las antenas falsas (también conocidas como *IMSI catchers* o *stingrays*) por parte de múltiples autoridades en México. La operación de estos sistemas se realiza sin ningún tipo de control judicial o administrativo. Además existe evidencia de su despliegue en zonas del centro histórico de la Ciudad de México en donde suelen ocurrir protestas, lo cual potencialmente implica la vigilancia e identificación de las personas asistentes.

Adicionalmente, recientemente se ha detectado el uso de otras formas de vigilancia masiva como la herramienta *Echo*, desarrollada por *Rayzone Group*, la cual permite a autoridades realizar búsquedas de información sobre personas en un sistema que recolecta masivamente información sobre personas usuarias de servicios y aplicaciones en Internet.

Este *outsourcing* de la vigilancia masiva constituye una novedosa manera de intentar eludir las limitaciones constitucionales a la vigilancia que el poder público puede ejercer sobre la población. Sin embargo, así como no resulta legítimo que el Estado construya y opere un sistema de vigilancia masiva sobre las población, mediante la recolección y sistematización de datos obtenidos de su navegación en sitios y aplicaciones en Internet, tampoco resulta compatible con las normas de derechos humanos delegar esa vigilancia masiva a particulares.

V. Control judicial inefectivo

Como ha sido explicado, el marco jurídico mexicano es claro en establecer un control judicial federal sobre las medidas de vigilancia de comunicaciones. Sin embargo, también ha sido documentado como este control judicial es frecuentemente eludido.

Las enormes discrepancias entre los datos estadísticos reportados por autoridades que llevan a cabo medidas de vigilancia, el Poder Judicial federal y empresas de telecomunicaciones son indicativos de una práctica generalizada de elusión del control judicial federal.

La evidencia también demuestra que el mecanismo excepcional contemplado en el artículo 303 del CNPP –para solicitar directamente el acceso a datos conservados a las empresas de telecomunicaciones sin control judicial previo y sujeto a la ratificación posterior por parte de la autoridad judicial federal– se ha convertido en la regla general y es frecuentemente abusado para eludir el control judicial efectivo.

Como la información estadística previamente detallada indica, la mayoría de las solicitudes de acceso a datos conservados no han contado con control judicial federal previo. Además, de aquellas en las que se han invocado las causales de excepción a las que se refiere el artículo 303 del CNPP, cerca del 40 por ciento no son ratificadas por la autoridad judicial federal, denotando su improcedencia original.

Aunado a ello, existen indicios adicionales de que un numero significativo de medidas de vigilancia en las que la autoridad alega causales de excepción al control judicial previo, ni siquiera son sometidas al proceso de ratificación judicial. Este *modus operandi*, como ha sido reportado, ha sido utilizado para la vigilancia ilegal.

Por si no fuera suficiente, el control judicial federal se ha hecho aún más improbable respecto de las medidas de vigilancia de comunicaciones desplegadas de manera autónoma por las autoridades, es decir, sin requerir la colaboración de empresas de telecomunicaciones y otros entes.

La utilización de *spyware* en contra de decenas de periodistas, personas defensoras de derechos humanos, funcionarios públicos y otras se ha llevado a cabo sin ningún tipo de control judicial. Lo mismo ha sucedido con herramientas como las antenas falsas, la geolocalización mediante sistemas como *Geomatrix* o *Echo*, e incluso en la operación de herramientas de extracción forense como *Cellebrite*.

La evidencia demuestra la facilidad con la que las autoridades pueden eludir el control judicial, las pocas posibilidades de que esa elusión sea detectada y las aún menores probabilidades de que ante la documentación de la vigilancia sin control judicial exista algún tipo de consecuencia.

Incluso en los casos en los que existe autorización judicial federal, no existe evidencia de que el Poder Judicial Federal ejerza efectivamente sus facultades de supervisión para evaluar si la implementación de las medidas de vigilancia se adecúan a los términos autorizados.

En resumen, las disposiciones normativas que disponen el control judicial federal previo o inmediato de las medidas de vigilancia, por sí solas no han garantizado un control judicial efectivo y requieren estar complementadas de otros sistemas de control para garantizar su efectividad práctica.

Sin control judicial efectivo, las autoridades con capacidades para llevar a cabo medidas de vigilancia cuentan con amplias garantías de que su utilización ilegal será difícilmente detectada y sancionada, fomentando así la continuación y repetición de los abusos.

VI. Ausencia de documentación y registro de actividades de vigilancia

La prevención, detección e impunidad de abusos en el despliegue de actividades de vigilancia de comunicaciones se encuentra importantemente obstaculizada por la ausencia de documentación y el ocultamiento deliberado de la misma.

La ausencia de documentación clave sobre los procesos de adquisición de equipos y sistemas de vigilancia y sobre las empresas que comercializan dichos productos y servicios, fomentan la corrupción, la adquisición y operación ilegal de los mismos y la dificultad de investigar a los responsables.

A pesar de que el marco jurídico establece la obligación de establecer registros de las intervenciones de comunicaciones privadas, las autoridades frecuentemente niegan la existencia de los mismos. La ausencia o inaccesibilidad de los registros constituye serios obstáculos para la supervisión de las medidas de vigilancia y la investigación de probables abusos. Esto se exacerba frente a la creciente proliferación de equipos y sistemas de vigilancia como 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.

Si bien fabricantes de este tipo de este tipo de tecnologías como *NSO Group* han afirmado que tecnologías de *spyware* como *Pegasus* poseen funcionalidades de registro (*logging*) que permiten la auditoría del sistema para identificar sus objetivos, autoridades han negado la existencia de dicho registro o señalado que no puede ser accedido sin colaboración del ente investigado, por lo que ni la autoridad judicial ni autoridades con facultades de investigación han sido capaces de acceder a estos registros.

Sin requisitos estrictos de registro de los equipos y sistemas utilizados para desplegar facultades de vigilancia, de las empresas que los desarrollan y comercializan, de las autoridades que los adquieren y utilizan, así como registros de uso y despliegue de medidas de vigilancia de comunicaciones, dichas medidas permanecerán siendo inverificables, con la consecuencia de perpetuar los abusos y la impunidad.

VII. Falta de transparencia

La transparencia permite el control social de la función pública, prevenir y detectar abusos, y otorga a las autoridades con facultades para investigarlos herramientas claves para evitar la impunidad de los mismos. Crucialmente, la transparencia también permite contar con evidencia para evaluar los riesgos y beneficios de determinadas políticas públicas. La transparencia respecto de medidas de vigilancia no es la excepción.

Aún cuando la vigilancia de comunicaciones se encuentra frecuentemente relacionada a actividades respecto de las cuales cierta secrecía resulta necesaria para su efectividad, como la seguridad pública, la investigación de delitos o la atención de amenazas a la seguridad nacional, ciertas medidas de transparencia respecto de estas actividades resultan cruciales 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.

Como ha sido expuesto, el marco jurídico mexicano –especialmente el artículo 70, fracción XLVII, de la LGTAIP– dispone medidas de transparencia estadística respecto de las medidas de vigilancia. De igual manera, órganos garantes en materia de transparencia y el Poder Judicial de la Federación han realizado interpretaciones que han permitido reconocer la publicidad de diversa información vinculada a medidas de vigilancia y abusos relacionados con estas. Sin embargo, persisten serios obstáculos para la efectividad de las medidas de transparencia.

A. El incumplimiento de las obligaciones de transparencia oficiosa establecidas en el artículo 70, fracción XLVII de la LGTAIP por parte de las autoridades que llevan a cabo medidas de vigilancia.

Como se ha documentado previamente,[283] existen graves incumplimientos a las obligaciones de transparencia oficiosa que establece el artículo 70, fracción XLVII de la LGTAIP.

De 2020 a 2023, únicamente dos autoridades federales (FGR y Guardia Nacional) y seis fiscalías estatales han publicado información estadística completa en la PNT respecto de medidas de intervención de comunicaciones privadas. Cuatro fiscalías estatales han publicado infor-

283. R3D, *Transparencia y Vigilancia*, 2019. Disponible en: https://r3d.mx/wp-content/uploads/TRANSPARENCIA-Y-VIGILANCIA-2019.pdf

mación incompleta. Otras autoridades federales como el Centro Nacional de Inteligencia y veintidós fiscalías estatales no han reportado información alguna a la PNT.

En el caso de información estadística sobre el acceso a datos conservados y geolocalización en tiempo real, únicamente dos autoridades federales y seis fiscalías estatales publicaron información estadística completa entre 2020 y 2023, mientras que otras once fiscalías estatales publicaron información incompleta en algunos trimestres. Otras autoridades federales y quince fiscalías estatales no reportaron información alguna a la PNT.

B. Información estadística incompleta y sin suficiente desagregación reportada a la PNT

Aún cuando las autoridades sí reportan información estadística a la PNT, existen varias circunstancias que reducen su utilidad y comparabilidad.

Por un lado, a pesar de que el marco jurídico mexicano establece la obligación de conservar registros fehacientes de las solicitudes de intervención de comunicaciones y de las decisiones judiciales relacionadas y que el artículo 70, fracciones XXX y XLVII, de la LGTAIP obligan a producir información estadística "*con la mayor desagregación posible*", la información que es efectivamente reportada a la PNT o entregada en respuesta a solicitudes de acceso a la información no cumple con dichos parámetros.

Frecuentemente algunas autoridades alegan no contar con la información estadística sobre medidas de vigilancia con el nivel de desagregación que se solicita. Es decir, diversas autoridades no conservan un registro "*fehaciente*" ni "*con la mayor desagregación posible*" de las solicitudes y resoluciones de autorización judicial en torno a medidas de vigilancia.

Los *Lineamientos técnicos generales para la publicación, homologación y estandarización de la información de las obligaciones establecidas en el título quinto y en la fracción IV del artículo 31 de la Ley General de Transparencia y Acceso a la Información Pública, que deben de difundir los sujetos obligados en los portales de Internet y en la Plataforma Nacional de Transparencia*,[284] publicados por el INAI, restringen de manera trascendental la efectividad de las obligaciones de transparencia oficiosa al limitar la obligación de reporte a que se refiere la fracción XLVII del artículo 70 de la LGTAIP al únicamente requerir que sea enlistada la información sobre medidas de vigilancia cuando las mismas se encuentren "*concluidas, es decir, que no formen parte de una investigación en curso*".

284. Disponible en: https://snt.org.mx/wp-content/uploads/Lineamientos-Tecnicos-Generales-Version-Integrada.pdf

Lo anterior reduce drásticamente la utilidad de las estadísticas reportadas pues no permite conocer el volumen de real de solicitudes. Esto se agrava dado el hecho de que, por ejemplo, según el Censo Nacional de Procuración de Justicia Estatal 2021 publicado por el INEGI, la inmensa mayoría de las carpetas de investigación no se encuentran concluidas.[285] Además, resulta contradictorio respecto a decisiones previas del INAI y de la SCJN, en torno a que el reporte de esta información estadística de ninguna manera puede considerarse que pone en riesgo ninguna investigación ni ningún interés público, como la procuración de justicia, la seguridad pública o la seguridad nacional.

De igual manera, los mencionados lineamientos agregan en el mismo campo estadístico la solicitudes de acceso a datos conservados y las de localización geográfica en tiempo real, lo cual de nuevo contraviene la obligación de "*mayor desagregación posible*" y reducen la utilidad y comparabilidad de la información estadística.

C. Ausencia e incomparabilidad de información estadística por parte del Poder Judicial de la Federación.

A pesar de que el artículo 70, fracción XLVII de la LGTAIP no excluye al Poder Judicial de la Federación (PJF) en el cumplimiento de la obligación de transparencia oficiosa en relación a estadísticas relacionadas a las solicitudes sobre medidas de vigilancia, el INAI recientemente dispuso excluir de su cumplimiento al PJF.

El INAI exime al Consejo de la Judicatura Federal (CJF) de la obligación de transparencia oficiosa contenida en el artículo 70, fracción XLVII de la LGTAIP a partir de la "*Modificación a la Tabla de aplicabilidad de las obligaciones de transparencia comunes de los sujetos obligados del ámbito federal, respecto de las obligaciones de transparencia a cargo del Consejo de la Judicatura Federal*", emitida por el INAI y publicada en el Diario Oficial de la Federación el 12 de julio de 2018.[286]

Esta modificación implica que no existe manera de contrastar la información aportada por las autoridades con facultades de vigilancia a la Plataforma Nacional de Transparencia (PNT) con la información que el PJF debería publicar en dicha plataforma, lo que resulta ser sumamente relevante en virtud de las inconsistencias entre las cifras reportadas por diversas autoridades que han sido desarrolladas previamente en este informe.

---

285. INEGI, Censo Nacional de Procuración de Justicia Estatal 2021. 19 de mayo de 2023. Disponibles en: https://www.inegi.org.mx/contenidos/programas/cnpje/2021/doc/cnpje_2021_resultados.pdf

286. Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5531037&fecha=12/07/2018

Si bien el CJF publica anualmente un informe estadístico sobre el número de asuntos que el Poder Judicial de la Federación conoce respecto de solicitudes de autorización judicial federal de medidas de vigilancia, como la intervención de comunicaciones privadas y el acceso a datos conservados por empresas de telecomunicaciones, dicha información carece de la especificidad y granularidad para hacerla comparable con otras fuentes de información. Destacadamente, dicha información no desagrega los datos por autoridad solicitante ni en los periodos de tiempo que permitirían contrastar con la información reportada por las propias autoridades solicitantes, lo cual de nuevo implica una violación al principio de "*máxima desagregación posible*".

D. La reserva absoluta de solicitudes y resoluciones relacionadas a la autorización de medidas de vigilancia, ante la ausencia de medidas de transparencia estadística suficientes y a las inconsistencias en su reporte.

Dado que existe amplia evidencia de inconsistencias entre la información estadística reportada por autoridades en la PNT, la información entregada a partir de solicitudes de acceso a la información, la información publicada -en su momento- por el IFT, así como ante la ausencia del cumplimiento de obligaciones de transparencia oficiosa con el máximo nivel de desagregación posible, se hace indispensable permitir a la sociedad acceder a las versiones públicas de las solicitudes y autorizaciones judiciales relacionadas a medidas de vigilancia, de manera que pueda contrastarse adicionalmente la información estadística reportada en el PNT o ante solicitudes de acceso a la información con la información que se desprende directamente de los documentos que son fuente de ese cálculo estadístico.

No obstante, persisten autoridades, e incluso órganos garantes, que pretenden establecer reservas absolutas en el acceso a los documentos de los que se puede desprender la veracidad o falsedad de las estadísticas reportadas.

Por ejemplo, el CJF, además de haber sido excluido arbitrariamente por el INAI del cumplimiento de las obligaciones de transparencia oficiosa a las que se refiere el artículo 70, fracción XLVII de la LGTAIP, y de no reportar información estadística con el máximo nivel de desagregación posible, ha considerado la reserva absoluta de la información, por lo que no aporta la información estadística necesaria ni permite a la sociedad generarla de manera propia a partir del acceso a las versiones públicas de las solicitudes y resoluciones.

Además, con la reserva absoluta de las resoluciones de los jueces de control en torno a las solicitudes de autorización respecto de medidas de vigilancia, se impide a la sociedad conocer la manera en la que el PJF interpreta las normas relacionadas a las medidas de vigilancia, con

lo que se le priva de conocer el contenido y alcance real de las medidas, lo cual resulta equivalente a no tener derecho a conocer las propias normas. Lo anterior contraviene además la obligación establecida en el artículo 73, fracción II de la LGTAIP la cual dispone la publicidad de "*las versiones públicas de todas las sentencias emitidas*" sin hacer distinción alguna.

Es importante resaltar que no se solicita acceso a los elementos fácticos de las solicitudes y resoluciones –como lo pueden ser nombres, números de teléfono u otros datos que identifiquen a las personas bajo investigación– ni a los hechos que las motivan, sino que únicamente se solicita acceso a versiones públicas, que testen la información sensible pero permitan conocer y calcular información estadística anonimizada y la manera en la que la autoridad judicial interpreta y define el contenido y alcance de las normas que regulan las medidas de vigilancia.

Por lo tanto, no es razonable la noción de que el acceso a versiones públicas de dichos documentos ponga en riesgo investigación alguna o los intereses de la procuración de justicia, seguridad pública o seguridad nacional.

E. La ausencia de obligaciones de transparencia para empresas que colaboran en materia de vigilancia

Al emitir los *Lineamientos de Colaboración en Materia de Seguridad y Justicia* publicados en el Diario Oficial de la Federación el 2 de diciembre de 2015,[287] el Instituto Federal de Telecomunicaciones contempló disposiciones encaminadas a favorecer la transparencia en la colaboración en materia de seguridad y justicia. En concreto, el Lineamiento Décimo Octavo de dichos Lineamientos estableció la obligación de las concesionarias y autorizadas de telecomunicaciones de entregar al IFT un informe semestral que debía contener información estadística como el número de requerimientos recibidos y cumplimentados de parte de autoridades facultadas, los cuales serían publicados por el Instituto en su portal de Internet.

La producción y publicación de estos informes durante los años 2016 y 2017 permitió al Instituto –y al público en general– conocer información relevante sobre las medidas de colaboración en materia de seguridad y justicia.

Por ejemplo, destaca que, entre los años 2016 y 2017, los concesionarios y autorizados de telecomunicaciones reportaron haber recibido poco más de 140 mil solicitudes de acceso a datos conservados y de geolocalización, de las cuales, en 97 por ciento de las ocasiones, la informa-

287. Lineamientos de Colaboración en Materia de Seguridad y Justicia. 2 de diciembre de 2015. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5418339&fecha=02/12/2015

ción fue entregada. Así mismo, 31.5 por ciento de las solicitudes reportadas –casi la tercera parte– fueron realizadas por autoridades sin facultades o cuya identidad no se conoce.[288]

De manera preocupante, los datos reportados revelan que las empresas Telcel y Telmex entregaron información en el 100 por ciento de las solicitudes recibidas (110,214 y 6,402, respectivamente), en tanto que Movistar otorgó los datos en 83.4 por ciento de las ocasiones; y AT&T, en 61.5 por ciento. Es importante destacar que el 31 por ciento de las solicitudes recibidas por Telcel (y entregadas en su totalidad) fueron efectuadas por autoridades sin facultades o no identificadas.[289]

No obstante la relevancia pública de la información contenida en los informes requeridos por el Instituto con base en los Lineamientos y de la utilidad para el ejercicio de las facultades propias del Instituto relacionadas con la protección del derecho a la privacidad, el Instituto decidió eliminar dichas obligaciones en abril de 2018,[290] por lo que hoy no es posible para el Instituto y para los usuarios conocer el número de solicitudes de acceso a usuarios que recibe cada concesionario o autorizado, las autoridades solicitantes o el número de solicitudes que son cumplidas o negadas por los concesionarios o autorizados.

Esta decisión inexplicable del IFT ha privado a la sociedad de la posibilidad de contrastar la información reportada por las empresas de telecomunicaciones con la información reportada por autoridades y por el Poder Judicial de la Federación. Aunado a esto, ha privado al IFT de información necesaria para ejercer sus facultades, como la establecida en el artículo 298, apartado D), fracción V de la LFTR, la cual otorga al Instituto la facultad imponer sanciones a los concesionarios o autorizados cuando no establezcan las medidas necesarias para garantizar la confidencialidad y privacidad de las comunicaciones de los usuarios.

Positivamente, en agosto de 2024, el IFT presentó un Anteproyecto de modificación a los Lineamientos en el que, entre otras cosas, reincorpora la obligación de producir informes estadísticos por parte de las empresas concesionarias en materia de telecomunicaciones. Sin embargo, al cierre de edición del presente informe, la modificación no ha sido materializada.

Finalmente, también debe señalarse que aunque algunas empresas proveedoras de aplicaciones, contenidos y servicios en Internet voluntariamente publican informes de transparencia en los que ofrecen alguna información estadística sobre las solicitudes provenientes de auto-

288. R3D. Quién No Defiende Tus Datos. 2018. Disponible en: https://r3d.mx/wp-content/uploads/R3D-QNDTD_digital.pdf

289. *Ídem*.

290. Modificación a los Lineamientos de Colaboración en Materia de Seguridad y Justicia. Publicada en el Diario Oficial de la Federación el 2 de abril de 2018. Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5517853&fecha=02/04/2018

ridades para el acceso a datos de personas usuarias, dicha información carece de granularidad y especificidad relevante para poder ser contrastada con otras fuentes de información.

F. La reserva excesiva de información y versiones públicas de documentos sobre aspectos técnicos de las herramientas y equipos utilizados para llevar a cabo medidas de vigilancia

Frecuentemente, las respuestas a solicitudes de acceso a la información relacionadas a documentos que forman parte de procesos de contratación relacionados a equipos y sistemas de vigilancia son reservadas de manera absoluta o excesiva.

Algunos precedentes del INAI,[291] otros órganos garantes,[292] e incluso en el Poder Judicial de la Federación[293] han reconocido que la reserva absoluta o excesiva de contratos y anexos técnicos relacionados a equipos y sistemas sobre la intervención de comunicaciones privadas viola el derecho de acceso a la información.

De parte de las autoridades y del INAI ha persistido la posición de que algunas categorías de información deben permanecer reservadas, en específico, las especificaciones técnicas de los equipos y sistemas adquiridos y los datos que identifican a los funcionarios que participan en los procesos de adquisición.

Desde nuestra perspectiva, la reserva de esas categorías de información obstaculiza de manera innecesaria el derecho de acceso a la información. Por ejemplo, respecto de las especificaciones técnicas de equipos y sistemas adquiridos, el análisis de parte de las autoridades y del INAI ha sido sumamente superficial, en tanto se asume que la revelación de dicha información, en todos los casos, reduce la efectividad o permite eludir los sistemas o equipos de intervención de comunicaciones cuando no se presenta ninguna evidencia de ello ni se realiza un análisis de dichas aseveraciones.

Por el contrario, las especificaciones técnicas de múltiples equipos y sistemas de intervención de comunicaciones privadas han sido publicados en el pasado sin que exista evidencia de que dichas publicaciones hayan reducido la efectividad de dichas herramientas.

---

291. *Véase* INAI. RRA 11072/19. Resolución del recurso de revisión interpuesto en contra de la respuesta del Centro Nacional de Inteligencia. 11 de diciembre de 2019.

292. Comisión Estatal de Garantía de Acceso a la Información Pública del Estado de San Luis Potosí. RRA 588/2017-3. Resolución del recurso de revisión interpuesto en contra de la respuesta de la Oficialía Mayor. 20 de octubre de 2017.

293. *Véase* Juzgado Octavo de Distrito en Materia Administrativa en la Ciudad de México. Juicio de Amparo 591/2018. Sentencia de 13 de diciembre de 2018. Disponible en: http://sise.cjf.gob.mx/SVP/word1.aspx?arch=729/072900002289871300130 12.docx_1&sec=Jos%C3%A9_Sebasti%C3%A1n___G%C3%B3mez_S%C3%A1mano&svp=1

Este es el caso relacionado con el *spyware Pegasus*, respecto del cual se conocen sus capacidad y características técnicas desde hace muchos años sin que dicho conocimiento haya frustrado de manera alguna su efectividad.

Es importante resaltar que el conocimiento de información técnica, en específico, las capacidades generales de los equipos y sistemas, es fundamental para que las personas podamos conocer las capacidades invasivas del Estado, así como evaluar y fiscalizar la pertinencia de la operación de dichas herramientas.

Igualmente, en múltiples solicitudes de acceso a la información, las autoridades únicamente reconocen la existencia de contratos y anexos técnicos, sin reconocer la existencia de documentación previa al contrato que, de conformidad con la legislación en la materia, debería existir dentro de un proceso de adquisición. En este sentido, se observa que tanto la ausencia de documentación de los procesos de adquisición y uso o, en su caso, la omisión en la entrega de las versiones públicas de dicha información afectan severamente la transparencia de dichos procesos de adquisición.

G. Avances en el reconocimiento de la publicidad de información indicios de abuso de las herramientas de vigilancia

Recientemente se han adoptado decisiones que han reconocido la publicidad de información relacionada a casos donde existen indicios y evidencia de abuso de equipos y sistemas para la vigilancia de comunicaciones.

Por ejemplo, el INAI ha emitido diversas resoluciones[294] en las que ha ordenado a la SEDENA entregar información sobre las contrataciones realizadas por dicha dependencia relacionadas con el *spyware Pegasus*. Igualmente, la SCJN reciente reconoció el interés público de información relacionada al *Caso Pegasus* en poder de la Unidad de Inteligencia Financiera.[295]

Es importante que los órganos garantes en materia de transparencia, así como el Poder Judicial continúen reconociendo que, como establece el artículo 115 de la LGTAIP, las reservas de información no son procedentes cuando se trate de violaciones graves a derechos humanos o de información relacionada con actos de corrupción, conceptos que resultan aplicables

294. *Véase*, por ejemplo: INAI, "Sedena debe informar sobre contrataciones con Comercializadora Antsua S.A. de C.V. para monitoreo de información remota". Nota Informativa INAI/010/23, 29 de enero de 2023. Disponible en: https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Nota%20INAI-010-23.pdf

295. SCJN, "Confirma la Corte resolución del INAI que ordena la entrega en versión pública de información relativa al Caso Pegasus", 6 de febrero de 2024. Disponible en: https://www.internet2.scjn.gob.mx/red2/comunicados/noticia.asp?id=7708

a los casos en los que existen indicios o evidencia de un uso ilegal de medidas de vigilancia de comunicaciones.

H. Incumplimiento de resoluciones

A pesar de los precedentes recientes en los que se ha dispuesto la publicidad de información contractual y financiera relacionada a la adquisición de equipos y sistemas de vigilancia respecto de los cuales existe evidencia de adquisición irregular o uso ilegal, las mismas no han permitido conseguir una mayor transparencia respecto de esos procesos debido al incumplimiento de las resoluciones.

Por ejemplo, como ha sido mencionado en este informe, a pesar de que el INAI ha emitido una resolución inatacable para la autoridad, ordenándole entregar los contratos relacionados al *spyware Pegasus*, la SEDENA se ha negado a cumplir con dicha resolución, e incluso ha impugnado una sentencia de amparo en la que un juez de distrito ha confirmado la obligatoriedad de la decisión.

Este ilegal e impune desacato de resoluciones de los órganos garantes en materia de transparencia atenta contra el derecho de acceso a la información pública, al mismo tiempo que demuestra la necesidad de que se establezcan mecanismos que permitan sancionar efectivamente estas conductas arbitrarias.

VIII. Ausencia de mecanismos de supervisión efectivos

A diferencia de la regulación existente en el derecho comparado, en México no existe un mecanismo de supervisión independiente explícitamente establecido para ejercer un control externo respecto del ejercicio de medidas de vigilancia. En su caso, el INAI posee ciertas facultades, a través de los procedimientos de verificación, para ejercer ciertas medidas de control, sin embargo, como ya ha sido adelantado, dichos procesos poseen diversas limitaciones y obstáculos.

Uno de los obstáculos más importantes es el plazo de duración máxima en la sustanciación de los procedimientos de verificación establecido en el artículo 149 de la Ley General de Protección de Datos en Posesión de Sujetos Obligados, el cual es aprovechado por las autoridades mediante medidas dilatorias, para complicar la labor del INAI en la sustanciación de dichos procedimientos, como ocurrió en el proceso de verificación INAI.3S.07.01-007/2018, en el que la entonces PGR fue encontrada en violación de sus obligaciones en materia de protección de datos personales.

Igualmente, los presupuestos de procedencia, las negativas de información aludiendo restricciones en materia de seguridad nacional, así como al carecer de medidas sancionatorias directas o suficientes, los efectos de dichos procedimientos son sumamente limitados y por ello no han sido efectivos para ejercer un control efectivo sobre las medidas de vigilancia estatal.

Como la Relatora Especial de la ONU sobre la lucha contra el terrorismo ha señalado, las decisiones sobre permitir el uso de *spyware* o las autorizaciones de exportación de los mismos, deben ir acompañadas de sólidas estrategias de debida diligencia para minimizar la posibilidad de daños derivados de esta potente e invasiva tecnología, así como de robustas funciones de registro y auditoría para que el uso indebido pueda investigarse, probarse y remediarse de forma eficaz. Estas auditorías deberán incluir algún mecanismos que permitan vincular en última instancia el *spyware* con sus productores y clientes gubernamentales, para que se pueda acceder a remedios adecuados en contra del productor o gobierno que los utiliza.[296]

Sin embargo, el marco jurídico mexicano no dispone de mecanismos de supervisión independientes, capaces de llevar a cabo auditorías aleatorias sobre las medidas de vigilancia, lo cual de nuevo fomenta su abuso y la impunidad.

IX. Impunidad

Como fue previamente detallado, en 2017, 2022 y 2023, las personas vigiladas por el *spyware Pegasus*, principalmente personas defensoras de derechos humanos y periodistas, presentaron denuncias penales ante la Fiscalía Especial para la Atención de Delitos Cometidos contra la Libertad de Expresión (FEADLE) por, entre otros, los delitos de intervención ilegal de comunicaciones privadas y acceso ilegal a sistemas informáticos. 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.

A pesar del llamado de múltiples instancias, nacionales e internacionales –como la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OACNUDH) y los Procedimientos Especiales de la ONU, la Comisión Interamericana de Derechos Humanos (CIDH)–sobre la necesidad de llevar a cabo una investigación diligente, con garantías de au-

296. Relatora Especial sobre la Lucha contra el Terrorismo, *Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach*, op. Cit. 28, pár. 59.
«Decisions to allow spyware use or spyware export approvals are obliged to be accompanied with robust due diligence strategies to minimize the potential for gender harms arising from this powerful and invasive technology, and robust record-keeping and audit functions so that misuse can be efficiently investigated, evidenced, and remedied. These audit functions ought to include some mechanism of digital watermarking such that spyware can ultimately be linked to its producer and their governmental client, with the result that avenues of remedy (against producer or governmental user) can be accessed.»

tonomía reforzadas, más de siete años después del anuncio del inicio de la primera carpeta de investigación, y a más de dos años del inicio de la investigación sobre la repetición del espionaje ilegal, ninguna persona ha sido condenada por los hechos.

La Fiscalía, entre otras deficiencias, se ha negado a realizar actos esenciales de investigación, ha obstruido y fragmentado las investigaciones, ha hecho recaer la carga de la prueba en las víctimas y les ha negado copia de los expedientes.[297]

La justicia y la rendición de cuentas también son obstruidas por las autoridades denunciadas, quienes afirman sistemáticamente que no existe ninguna base de datos o documentación formal de los registros relativos a las personas o números atacados, a pesar de evidencia en contrario. En 2019, el Instituto Nacional de Acceso a la Información y Protección de Datos Personales (INAI) determinó que la Fiscalía había incumplido sus obligaciones conforme a la legislación de Protección de Datos Personales al ocultar contratos con *NSO Group*.[298] Sin embargo, hasta la fecha, la Fiscalía General se ha negado a emprender cualquier investigación seria e independiente en relación con la obstrucción de la justicia documentada.

Varias investigaciones aún no han dado señales de progreso. La única detención de una persona[299] –a quien se le imputó el delito de intervención telefónica por su probable participación como operador del software dentro de una de las empresas intermediarias entre *NSO Group* y la PGR– solo fue posible gracias a información proporcionada por una de las víctimas, que remitió a las autoridades a la red de intermediarios que comercializaba *Pegasus* en México.

A pesar de que se celebró un juicio en diciembre de 2023 contra dicho operador, en donde se confirmó mediante sentencia judicial la ilegal intervención de comunicaciones en contra de la periodista Carmen Aristegui, no han existido avances en la imputación de responsabilidades de funcionarios públicos de las dependencias como la PGR, el CISEN y el Ejército Mexicano, respecto de las cuales existe amplia evidencia de haber adquirido y operado el spyware.

---

297. Carpeta de investigación FEADLE FED/SDHPDSC/UNAI-CDMX/0000430/2017; Ahmed, Azam, "Mexico Spyware Inquiry Bogs Down. Skeptics Aren't Surprised", *The New York Times*, 20 de febrero de 2018, disponible en: https://www.nytimes.com/2018/02/20/world/americas/mexico-spyware-investigation.html; R3D: Red en Defensa de los Derechos Digitales, "A un año de #GobiernoEspía, prevalece la impunidad", 20 de junio de 2018, disponible en: https://r3d.mx/2018/06/20/comunicado-a-un-ano-de-gobiernoespia-prevalece-la-impunidad/

298. INAI, "Determina INAI que FGR, respecto al software *Pegasus*, incumplió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados", 20 de febrero de 2019, disponible en: https://inicio.inai.org.mx/Comunicados/Comunicado%20INAI-054-19.pdf

299. *Article 19 MX-CA*, "Avance del caso Pegasus en México debe ser un punto de no retorno que ayude a esclarecer un crimen de talla mundial", 8 de noviembre de 2021, disponible en: https://articulo19.org/avance-del-caso-pegasus-en-mexico-debe-ser-un-punto-de-no-retorno-que-ayude-a-esclarecer-un-crimen-de-talla-mundial/%20; *Aristegui Noticias*, "Detiene FGR a uno de los involucrados en espionaje con Pegasus", 8 de noviembre de 2021, disponible en: https://aristeguinoticias.com/0811/mexico/detiene-fgr-a-uno-de-los-involucrados-en-espionaje-con-pegasus/

La renuencia de la Fiscalía a realizar diligencias en cuanto a líneas de investigación respecto de la Agencia de Investigación Criminal de la FGR demuestra la falta de autonomía, imparcialidad y profesionalismo en la investigación, máxime cuando tanto la autoridad que realiza la investigación, la FEADLE, como la única autoridad que ha admitido el uso del *malware Pegasus*, la AIC, forman parte de la misma Fiscalía General. Así mismo, no se han llevado a cabo acciones de investigación serias respecto al CISEN ni al Ejército Mexicano, con evidencias que los confirman como operadores de *Pegasus* durante el gobierno de Enrique Peña Nieto.

Respecto a la más reciente investigación sobre el abuso de *Pegasus* por parte del Ejército entre 2019 y 2022, la Fiscalía no ha logrado ningún avance en más de dos años. Ni siquiera ha podido obtener los contratos en los que el Ejército obtuvo licencias para operar *Pegasus*. La SEDENA se ha negado a hacer públicos los contratos con *NSO Group* para la adquisición de *Pegasus* u otros sistemas de vigilancia, como prometió públicamente el Presidente López Obrador,[300] a pesar de las numerosas pruebas y documentos que muestran el número y las fechas de los contratos, así como los pagos realizados por la SEDENA.

A pesar de la gravedad de las denuncias, México no ha aceptado el establecimiento de un mecanismo internacional de supervisión independiente y los documentos relacionados con la contratación y uso de Pegasus aún no han sido hechos públicos por las autoridades del Estado mexicano. El gobierno no sólo ha faltado a su obligación de garantizar la verdad y justicia a las víctimas, sino que ha perpetuado la impunidad y generado las condiciones para la repetición de los hechos.

La impunidad también prevalece en otros casos de vigilancia ilegal, como el acceso ilegal a datos conservados por empresas de telecomunicaciones en perjuicio de la periodista Marcela Turati, la antropóloga forense Mercedes Doretti y la defensora de derechos humanos Ana Lorena Delgadillo, ni las decenas de personas cuyos datos fueron indebidamente accedidos por las Fiscalías de la Ciudad de México y Colima, simulando su relevancia para en investigaciones sobre secuestro.

No existe ninguna investigación abierta en torno al uso de herramientas de vigilancia masiva, como las antenas falsas o las herramientas de outsourcing de vigilancia masiva, ni el documentado uso ilegal de la herramienta de geolocalización *Geomatrix*, otras tecnologías de *spyware* como las desarrolladas por la empresa *Hacking Team*, ni se ha indagado sobre los indicios de utilización de herramientas de vigilancia de manera previa a los homicidios de los periodistas Cecilio Pineda Brito y Freddy Román Román.

300. R3D: Red en Defensa de los Derechos Digitales, "Persisten interrogantes respecto de la información presentada por la SSPC sobre la adquisición y uso de Pegasus", 29 de julio de 2021, disponible en: https://r3d.mx/2021/07/29/interrogantes-sspc-pegasus/

La rampante impunidad por la corrupción en la adquisición de equipos y sistemas de vigilancia, por el espionaje ilegal a través de las mismas, así como por la conductas de encubrimiento y obstrucción de justicia ha generado un clima propicio para el abuso.

La ausencia absoluta de medidas que fomenten la prevención de abusos, la improbabilidad de la detección de los mismos y la prácticamente garantizada impunidad aún en los casos en los que irregularidades son detectadas demuestra que la vigilancia continúa fuera de control y que los casos de abuso se seguirán repitiendo y agravando si no se adoptan medidas profundas de reforma para establecer controles democráticos a la vigilancia de comunicaciones en México.

CAPÍTULO CINCO

Propuestas para el establecimiento de controles democráticos a la vigilancia

A partir del diagnóstico presentado, se considera indispensable el rediseño e implementación de una reforma profunda al marco jurídico e institucional en México, de manera que las facultades de vigilancia de comunicaciones en México –en cumplimiento de las recomendaciones y estándares internacionales– posean suficientes controles democráticos para prevenir, detectar y remediar abusos, evitar la corrupción y garantizar la verdad y justicia.

I. Moratoria sobre la venta, transferencia y uso de tecnologías de vigilancia

En línea con lo que ha sostenido la Oficina de la Alta Comisionada de las Naciones Unidas para los Derechos Humanos (OACNUDH),[301] la Comisión Interamericana de Derechos Humanos (CIDH),[302] así como los relatores para la libertad de expresión de la ONU[303] y la CIDH, se reitera el llamado a la moratoria inmediata sobre la venta, la transferencia y el uso de la tecnología de vigilancia hasta tanto se establezcan marcos normativos en línea con los derechos humanos.

II. Impulso de reformas legales y administrativas que establezcan controles democráticos a la vigilancia estatal

301. OACNUDH, "Declaración de la Alta Comisionada de la ONU para los Derechos Humanos, Michelle Bachelet, sobre el uso de software espía para vigilar periodistas y personas defensoras de derechos humanos", 19 de julio de 2021, disponible en: https://hchr.org.mx/comunicados/declaracion-de-la-alta-comisionada-de-la-onu-para-los-derechos-humanos-michelle-bachelet-sobre-el-uso-de-software-espia-para-vigilar-periodistas-y-personas-defensoras-de-derechos-humanos/

302. CIDH, "La CIDH, RELE y OACNUDH expresan preocupación ante los hallazgos sobre uso del software Pegasus para espiar a periodistas y organizaciones de la sociedad civil en El Salvador", 31 de enero de 2022. Disponible en: http://www.oas.org/es/cidh/jsForm/?File=/es/cidh/prensa/comunicados/2022/022.asp

303. OHCHR, "Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech", 12 de agosto de 2021. Disponible en: https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening?LangID=E&NewsID=27379

Adicionalmente a los llamados realizados por diversos organismos internacionales para la adopción de marcos normativos capaces de controlar a las tecnologías de vigilancia que acompañan el llamado a la moratoria sobre su comercialización y uso, existen recomendaciones específicas dirigidas al Estado Mexicano.

Frente a la evidencia del abuso generalizado y sistemático de la vigilancia en México, en el Informe conjunto del Relator Especial para la libertad de expresión de la CIDH y el Relator Especial de las Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y de expresión sobre su misión a México, publicado en Junio de 2018, se realizó la siguiente recomendación:

> *89. Los Relatores Especiales instan a las autoridades a adoptar las siguientes medidas:*
> *[...]*
> *(b) Establecer un marco legal para proteger a personas de intromisiones arbitrarias o clandestinas en su privacidad, incluida la protección de las fuentes periodísticas conforme a los estándares internacionales sobre la materia. Se deben establecer garantías y medidas de supervisión judicial de los organismos estatales implicados en vigilancia, dentro de los límites permisibles en una sociedad democrática. México debería considerar la posibilidad de crear un órgano independiente para supervisar de manera eficaz las tareas de vigilancia del Estado.*

En este sentido, para la implementación de estas recomendaciones se propone una serie de reformas que, adicionalmente a lo ya señalado respecto de la adquisición de sistemas de vigilancia, persiguen tres objetivos fundamentales:

I. Prevenir o evitar el abuso de medidas de vigilancia.
II. Detectar el abuso de medidas de vigilancia.
III. Sancionar y remediar los abusos de medidas de vigilancia.

A continuación se presenta un resumen de las propuestas contenidas en la **"*Propuesta de reformas para el establecimiento de controles democráticos a la vigilancia de comunicaciones*"** que puede ser consultada como **Anexo**[304] al presente informe.

Para efectos de este Capítulo, se entiende que las medidas de vigilancia incluyen la intervención de comunicaciones privadas, el acceso a datos conservados, la localización geográfica en tiempo real de dispositivos y la extracción de información de dispositivos.

304. Disponible en: https://r3d.mx/reforma-vigilancia/

A. Definición clara, precisa y detallada de las autoridades facultadas, el procedimiento y circunstancias en las que pueden llevarse a cabo medidas de vigilancia.

Con el objetivo de evitar la incertidumbre jurídica y la discrecionalidad en el despliegue de medidas de vigilancia, es necesario establecer con mayor explicitud aspectos fundamentales, como la identificación de las autoridades facultadas, la exclusividad de la competencia de la autoridad judicial federal para conocer de las solicitudes en la materia, así como delimitar y orientar 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, garantizando así una mayor previsibilidad sobre los alcances de estas medidas.

Para ello, deben modificarse diversas disposiciones como el Código Nacional de Procedimientos Penales (CNPP), la Ley de Seguridad Nacional (LSN), la Ley de la Guardia Nacional (LGN), el Código Militar de Procedimientos Penales (CMPP), la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR), la Ley Orgánica del Poder Judicial Federal (LOPJF) y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), entre otras disposiciones, para establecer con claridad, precisión y detalle lo siguiente:

I. Debe **definirse con absoluta precisión y claridad qué autoridades se encuentran facultadas** para llevar a cabo medidas de vigilancia, **incluyendo aquellas que no requieren colaboración de algún concesionario o proveedor**, así como los **casos y circunstancias en las que la autoridad judicial federal podrá autorizarlas**. Al hacerlo, deben observarse los límites subjetivos y materiales que establece el artículo 16 constitucional. Es decir, únicamente pueden considerarse autoridades facultadas, aquellas autoridades federales facultadas explícitamente por una ley, así como los titulares del Ministerio Público de cada entidad federativa; y no podrán autorizarse medidas de vigilancia relacionadas a materias carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor.

II. Se debe reconocer de manera explícita que las medidas de vigilancia solamente podrán ser autorizadas por una **autoridad judicial federal** cuando sea una medida **idónea, necesaria y proporcional**. Lo anterior implica exigir, como mínimo, estándares probatorios mínimos que justifiquen la autorización de las medidas, como lo es el **estándar de "causa probable"**.

III. Deben **prohibirse de manera expresa las medidas de vigilancia masiva** y las medidas de vigilancia que **comprometan masivamente la integridad y seguridad de sistemas de comunicación**.

B. Registro y control de proveedores de tecnologías de vigilancia

México carece de regulación efectiva de los procesos de adquisición de equipos y sistemas de vigilancia de comunicaciones. La ausencia de regulación de la industria que desarrolla y comercializa herramientas de vigilancia incrementa el riesgo de su adquisición por parte de entes no autorizados; facilita la discrecionalidad, los sobrecostos y la corrupción; exacerba los riesgos de despliegue de medidas de vigilancia ilegales; y genera obstáculos para que las autoridades con facultades de supervisión e investigación lleven a cabo su crucial labor para prevenir, detectar y remediar abusos.

Por ello, se propone el establecimiento de las siguientes medidas:

I. Establecimiento de un registro de proveedores

Resulta indispensable establecer un registro de proveedores de equipos y sistemas de vigilancia de comunicaciones que permita contar con un control respecto de las personas que comercializan tecnologías de vigilancia. Este registro debe incluir datos de identificación del nombre o razón social del proveedor, datos de contacto, catálogo de equipos y sistemas de vigilancia de comunicaciones que el proveedor comercializa, datos de identificación del fabricante o desarrollador de los productos o servicios, así como el país de origen de los mismos.

Esta información resulta útil para que las autoridades facultadas para adquirir y desplegar medidas de vigilancia de comunicaciones puedan identificar potenciales proveedores y disminuir la discrecionalidad y el dispendio de recursos públicos. Así mismo, constituye información de suma relevancia para que autoridades con facultades de investigación, fiscalización y auditoría puedan indagar casos de abuso.

II. Requisitos de inscripción orientados a garantizar la cooperación con investigaciones

Con el objetivo de evitar que, argumentando impedimentos legales o contractuales, algún proveedor alegue la imposibilidad de cooperar con investigaciones, resulta necesario establecer como requisito para la inscripción en el registro que los proveedores manifiesten la ausencia de impedimentos de esa naturaleza.

Este requisito, por un lado, permite garantizar la cooperación ante la investigación de potenciales abusos, y también contribuye a incentivar que otras jurisdicciones en las que los equipos y sistemas de vigilancia son desarrollados modifiquen los impedimentos para dicha colaboración, ante el riesgo de que su industria se vea marginada de mercados importantes como el mexicano.

III. Requisitos de inscripción orientados a proteger los derechos humanos

De manera similar a la propuesta anterior, el proceso de registro de proveedores ofrece una oportunidad para que México, en cumplimiento de su obligación de proteger derechos humanos, a la luz de los Principios Rectores sobre las Empresas y los Derechos Humanos, evite contribuir a violaciones a derechos humanos en las que proveedores de equipos y sistemas de vigilancia tengan alguna participación.

Para ello, la regulación debe establecer como impedimento para la inscripción en el registro de proveedores el que los mismos, así como sus subsidiarias y filiales o las personas fabricantes o desarrolladoras de los equipos y sistemas de vigilancia, comercialicen sus productos o servicios en países donde se cometan violaciones sistemáticas a los derechos humanos.

Para determinar lo anterior, sería deseable que alguna dependencia, como lo podría ser la Secretaría de Relaciones Exteriores o la Secretaría de Economía, mantenga una lista de personas físicas o morales que considere deben ser restringidas, de manera similar a como lo hace el Departamento de Comercio de los Estados Unidos.[305]

IV. Requisitos de inscripción orientados a proteger la seguridad nacional

La adquisición de tecnologías avanzadas de vigilancia también pueden conllevar riesgos a la seguridad nacional, en tanto puede contener puertas traseras (*backdoors*) u otras características que permitan a una entidad extranjera explotar vulnerabilidades en perjuicio de los intereses legítimos de México.

El procedimiento de registro de proveedores ofrece una oportunidad para que el Estado mexicano pueda atender los riesgos a la seguridad nacional, señalando como impedimento para el registro que los proveedores, así como sus subsidiarias y filiales o las personas fabricantes o desarrolladoras de los equipos y sistemas de vigilancia, se considere que amenazan la seguridad nacional del país.

Para ello, es deseable utilizar el mismo mecanismo propuesto anteriormente, en el que alguna dependencia, como podría ser la Secretaría de Relaciones Exteriores, la Secretaría de Economía, el Centro Nacional de Inteligencia o el Consejo de Seguridad Nacional, mantenga una lista de personas físicas o morales que considere deben ser restringidas, de manera similar a como

305. Departamento de Comercio de los Estados Unidos, Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities, 3 de noviembre de 2021. Disponible en: https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list

lo hace el Departamento de Comercio de los Estados Unidos o a través de órdenes ejecutivas por parte de la Presidencia de los Estados Unidos.[306]

C. Registro y control en los procesos de adquisición de equipos y sistemas de vigilancia

Los procesos de adquisición de equipos y sistemas de vigilancia deben regularse de manera específica con el objetivo de que dichas tecnologías no sean adquiridas de manera ilegal, por ejemplo, al ser tecnologías con capacidades que exceden los principios de necesidad y proporcionalidad o al pretender ser adquiridas por entes no facultados. La estricta documentación de estos procedimientos también ofrece elementos para prevenir actos de corrupción y permitir la detección, investigación y sanción de cualquier irregularidad.

Para este fin, se propone establecer procedimientos en los que, dentro de los requisitos previos a la adquisición de este tipo de tecnologías, se exiga la obtención de una autorización por parte de alguna dependencia ajena a la contratación.

Dicha dependencia deberá asegurarse, por ejemplo, que la autoridad contratante cuente con facultades legales para llevar a cabo medidas de vigilancia; que los proveedores se encuentren registrados, cumplan con todos los requisitos y no se ubiquen en las causales de impedimento desarrolladas previamente; y que las tecnologías adquiridas cumplan con diversos parámetros para asegurar su legalidad y permitir la trazabilidad de su uso.

En este sentido, la regulación debe asegurarse de que la tecnología que pretende ser adquirida:

I. **No constituye una tecnología de vigilancia masiva.** Es decir, su despliegue únicamente afecta de manera focalizada al objetivo de vigilancia y no compromete masivamente la integridad y seguridad de los sistemas de comunicación.

II. **Es comercializada o desarrollada por una persona registrada en el registro de proveedores.** Incluyendo verificar que no existen impedimentos legales o contractuales para la colaboración con autoridades competentes para investigar conductas relacionadas al uso ilegal de los equipos o sistemas de vigilancia.

III. **Es comercializada o desarrollada por una persona que no se encuentra incluída en la lista de personas impedidas.** Por ejemplo, por su participación en la comisión de viola-

306. Oficina de la Presidencia de los Estados Unidos, Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security, 27 de marzo de 2023. Disponible en: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security/

ciones graves a los derechos humanos o por constituir amenazas a la seguridad nacional.

IV. **Posee mecanismos que garantizan la rendición de cuentas.** Deben establecerse requisitos de diseño que incluyan medidas como los registros de auditoría inalterables, la inclusión de huellas digitales (fingerprinting) y otros mecanismos de seguridad que permitan detectar, trazar e investigar los usos de la tecnología.

Adicionalmente, la regulación debe establecer un registro de equipos y sistemas tecnológicos de vigilancia que contenga información que identifique a las dependencias que cuentan con estas herramientas, los proveedores y desarrolladores, los nombres comerciales de las mismas, las fechas de contratación, su vigencia, entre otra información relevante.

Para ello, se sugiere la inclusión de información sobre los equipos y sistemas tecnológicos de vigilancia adquiridos y utilizados por las autoridades competentes en el Registro Nacional de Armamento y Equipo al que se refiere el artículo 154 de la Ley General del Sistema Nacional de Seguridad Pública o en otro registro incorporado a una ley o disposición administrativa.

La existencia de este registro es crucial para permitir que las autoridades competentes para investigar, fiscalizar y auditar la adquisición y uso de estos sistemas, cuente con elemento suficientes para llevar a cabo su labor, inhibiendo así casos de abuso y permitiendo, en todo caso, su detección, investigación y sanción.

D. Registro y control del despliegue de medidas de vigilancia

En cumplimiento de las obligaciones constitucionales y legales existentes que disponen la existencia de registros de las medidas de vigilancia llevadas a cabo, es necesario establecer mecanismos de control y registro sobre el uso de medidas de vigilancia, de manera que queden asentadas de manera pormenorizada e inmutable las medidas de vigilancia encubierta que sean llevadas a cabo por las autoridades competentes.

En concreto se sugiere establecer:

I. **Requisitos e identificación de agentes que participan en la toma de decisiones y operación de sistemas de vigilancia:** Establecer requisitos de certificación, evaluaciones de control de confianza y mantener un registro pormenorizado de los agentes que hayan sido capacitados y que participen en la implementación de medidas de vigilancia.

II. **Registros de uso:** Establecer mecanismos que garanticen el registro pormenorizado de la utilización de medidas de vigilancia, incluyendo los agentes participantes, los sujetos, métodos utilizados y otros datos necesarios para identificar cada uso de medidas de vigilancia.

III. **Mecanismos para prevenir el uso no registrado de sistemas de vigilancia o la alteración del registro:** Establecer la obligación de implementar medidas técnicas y administrativas para prevenir usos no registrados de sistemas de vigilancia o alteraciones en el registro de uso.

E. Control judicial efectivo

Con el objetivo de garantizar la efectividad del control judicial sobre las medidas de vigilancia, es indispensable fortalecer las medidas de control judicial existentes de la siguiente manera:

I. **Exclusiva competencia federal:** A partir de los precedentes judiciales que así lo han establecido, resulta necesario armonizar la legislación, por ejemplo el artículo 303 del CNPP, para establecer de manera inequívoca que únicamente la autoridad judicial federal es competente para conocer y resolver de solicitudes de autorización de medidas de vigilancia, incluyendo el acceso a datos conservados y la localización geográfica en tiempo real.

II. **Registro de control judicial:** Establecer mecanismos que garanticen el registro pormenorizado de de medidas de vigilancia cuya autorización es solicitada u otorgada por el Poder Judicial de la Federación, incluyendo las autoridades solicitantes, los sujetos, los métodos, sistemas o herramientas utilizadas, en su caso, los concesionarios, autorizados o proveedores que deban prestar alguna colaboración y otros datos necesarios para identificar cada uso de medidas de vigilancia.

III. **Modificación del mecanismo excepcional establecido en el artículo 303 del CNPP:** Es necesario reformular los mecanismos de emergencia contemplados en el CNPP, de manera que la solicitud de ratificación de medidas de vigilancia deba ser enviada al Juez de Control competente de manera simultánea a cualquier requerimiento a un concesionario, autorizado o proveedor o al inicio de la medida misma. Igualmente, debe establecerse el procedimiento a seguir cuando la orden de ratificación sea negada, el cual debe incluir la notificación a la persona afectada y procedimientos disciplinarios adecuados.

IV. **Supervisión de las medidas:** Es necesario fortalecer las capacidades de supervisión de medidas de vigilancia autorizadas por parte de la autoridad judicial que otorgue dicha autorización. Para ello es necesario contemplar mecanismos técnicos y administrativos que permitan que dicha supervisión sea desarrollada de manera autónoma, inclusive sin necesidad de cooperación o conocimiento de parte de la autoridad que lleva a cabo las medidas de vigilancia. Por ejemplo, permitiendo a la autoridad judicial el acceso autónomo a los registros de auditoría de las herramientas de vigilancia utilizadas.

F. Reconocimiento del derecho de notificación

Con el objeto de inhibir instancias de abuso y garantizar que las personas afectadas por medidas de vigilancia cuentan con la posibilidad de ejercer su derecho de acceso a la justicia, es necesario reconocer el derecho de notificación de las personas que son objeto de medidas de vigilancia. Es decir, 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, como es establecido en el derecho comparado, dicha notificación puede no poder llevarse a cabo de manera previa o inmediata, en tanto se podría obstaculizar el éxito de una investigación legítima, dicha notificación puede llevarse a cabo de manera diferida, cuando 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.

En concreto se propone:

I. Regular la **obligación de notificar** a las personas que hayan sido sujetas a una medida de vigilancia.

II. Establecer el **control judicial de este proceso y la posibilidad de diferir la notificación**, por un tiempo determinado, cuando sea necesario para evitar el peligro de fuga, la destrucción de evidencia o un riesgo inminente a la vida o integridad de una persona.

III. Se debe establecer la **obligación de colaboración** de parte de concesionarios y autorizados para prestar servicios de telecomunicaciones, así como a proveedores de aplicaciones, contenidos y servicios en Internet respecto de la colaboración con autoridades de seguridad y justicia para llevar a cabo la notificación correspondiente.

IV. La **notificación debe incluir información relevante** como la autoridad que llevo a cabo la medida, su duración, así como acceso a la información que fue obtenida.

G. Fortalecimiento de las facultades de fiscalización, auditoría y supervisión independiente de medidas de vigilancia

En concordancia con la experiencia internacional, se propone el establecimiento de un mecanismo de supervisión independiente a las tareas de vigilancia de comunicaciones, mediante la creación de un órgano de supervisión independiente o en su defecto el desarrollo de dichas facultades dentro del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). En concreto se sugiere:

I. Otorgar facultades al órgano supervisor independiente para realizar **procedimientos de vigilancia, auditoría o verificación oficiosa**, incluyendo de manera aleatoria, para verificar el cumplimiento de las disposiciones que regulan las medidas de vigilancia.

II. Reconocer explícitamente la **facultad de acceder y requerir a cualquier autoridad cualquier información** necesaria para llevar a cabo su función de supervisión, incluyendo información reservada. También debe incluirse la facultad de requerir información a particulares que presten colaboración a autoridades para llevar a cabo medidas de vigilancia encubierta.

III. Establecer la obligación de producir un **informe periódico y público** sobre los hallazgos y recomendaciones del órgano supervisor.

H. Transparencia efectiva

A partir del diagnóstico presentado, es necesario adoptar disposiciones que permitan contar con medidas de transparencia efectiva para prevenir, detectar y remediar instancias de abuso. Para ello, es necesario contar con información estadística con suficiente granularidad y comparabilidad de manera que sea posible evaluar la efectividad de las medidas y detectar posibles irregularidades.

Igualmente, es necesario garantizar el acceso a información suficiente sobre los equipos y sistemas de vigilancia utilizados y sobre los procesos de autorización de las medidas, de manera que la sociedad pueda conocer y evaluar de manera general el alcance y pertinencia de las medidas de vigilancia y de las normas que las regulan.

I. Reformas legales en materia de transparencia

La mayoría de los objetivos en materia de transparencia pueden ser conseguidos sin necesidad de reformas legales, sin embargo resultaría útil llevar a cabo reformas que hagan explícitos los precedentes de interpretación administrativa y judicial vigentes. Por ejemplo, sería deseable mejorar redacción de la fracción XLVII del artículo 70 de la LGTAIP, para establecer con mayor claridad los sujetos obligados y el nivel de desagregación que debe ser reportado como parte de las obligaciones de transparencia oficiosa.

Igualmente, sería ideal realizar otras reformas a la Ley Federal de Telecomunicaciones y Radiodifusión, al Código Nacional de Procedimientos Penales, la Ley de Seguridad Nacional, la Ley de la Guardia Nacional, entre otras, para explicitar, como ha sido interpretado por la SCJN, que no pueden invocarse disposiciones en dichos ordenamientos para impedir de manera absoluta y automática el acceso a la información en las materias de procuración de justicia, seguridad pública o seguridad nacional, sin atenerse a los principios de transparencia y acceso

a la información pública establecidos en la LGTAIP, especialmente cuando existen indicios de posibles violaciones a derechos humanos o actos de corrupción.

II. Modificación de disposiciones administrativas por parte del INAI

Un número importante de objetivos de transparencia pueden ser conseguidos a partir de la modificación de disposiciones administrativas a cargo del INAI, como los "*Lineamientos técnicos generales para la publicación, homologación y estandarización de la información de las obligaciones establecidas en el título quinto y en la fracción IV del artículo 31 de la Ley General de Transparencia y Acceso a la Información Pública, que deben de difundir los sujetos obligados en los portales de Internet y en la Plataforma Nacional de Transparencia*" de manera que sean incorporado lo siguientes:

I. Inclusión de estadísticas sobre "investigaciones en curso". Debe eliminarse cualquier referencia a que la obligación de reporte de información estadística oficiosa, según el artículo 70, fracción XLVII de la LGTAIP, no comprende aquélla relacionada a "investigaciones en curso". Reportar información estadística completa, incluyendo la que se encuentra "en curso" no pone en riesgo de manera alguna dichas investigaciones.

II. Inclusión de nuevos criterios sustantivos de contenido y modificación de formatos. Deben incluirse criterios sustantivos adicionales para el cumplimiento de la obligación de transparencia oficiosa. Entre los criterios que deben agregarse debe incluirse:

a) Identificar si la medida de vigilancia se realiza de manera autónoma o con colaboración de algún concesionario, autorizado o proveedor.

b) En su caso, identificar el concesionario, autorizado o proveedor que preste colaboración para llevar a cabo la medida de vigilancia.

c) En los casos de acceso a datos conservados o geolocalización en tiempo real, identificar si se lleva a cabo la medida en los casos de emergencia señalados en el artículo 303 del CNPP, es decir, sin autorización judicial previa.

d) En los casos de emergencia, identificar si la solicitud de ratificación judicial fue autorizada o negada.

e) Identificar el número (cantidad) de personas y/o dispositivos respecto de los cuáles se lleva a cabo la medida de vigilancia.

f) En el caso de las medidas de vigilancia llevadas a cabo por fiscalías, Identificar el estado de la carpeta de investigación o expediente de investigación. En el caso de carpetas de investigación, si la carpeta de investigación se encuentra abierta, se ejerció acción penal, se concluyó con no ejercicio de acción penal o improcedencia, reserva o archivo, incompetencia u otra determinación y/o conclusión.

g) Establecer criterios y formatos específicos para el reporte de parte del Consejo de la Judicatura Federal que hagan comparables los reportes de autoridades con los reportes del CJF.

En correspondencia con dichos criterios, es necesario modificar los formatos correspondientes. Además es necesario asegurar que esta información sea ofrecida en un formato que permita su reutilización por los usuarios y por las máquinas, es decir, presentarse mediante el enfoque de datos abiertos, lo cual implica facilitar la posibilidad de exportar el conjunto de datos publicados en formatos estructurados para facilitar el consumo e interpretación.

Otra disposición administrativa que debe modificarse es la "*Tabla de aplicabilidad de las obligaciones de transparencia comunes de los sujetos obligados del ámbito federal, respecto de las obligaciones de transparencia a cargo del Consejo de la Judicatura Federal*" de manera que el Consejo de la Judicatura Federal vuelva a considerarse obligado para reportar estadísticas respecto de las solicitudes de autorización y ratificación relacionadas a medidas de vigilancia.

Lo anterior permitirá hacer comparable la información reportada por las autoridades facultadas y aquélla reportada por el Poder Judicial Federal, posibilitando así la detección de irregularidades.

III. Modificación de disposiciones administrativas por parte del CJF

Debe modificarse el "A*cuerdo General del Pleno del Consejo de la Judicatura Federal, que regula la asignación de audiencias y asuntos, la rendición de estadística y los libros electrónicos de control en los Centros de Justicia Penal Federal*" de manera que se establezcan obligaciones de registro estadístico compatibles con la obligación de transparencia oficiosa establecida en el artículo 70, fracción XLVII de la LGTAIP.

Específicamente se sugiere modificar lo relacionado a los libros de control obligatorios para el registro de las actuaciones de los jueces de control de los Centros de Justicia Penal Federal, en concreto el artículo 14 del Acuerdo, referente al libro dos (libro de actos de investigación con control judicial) de manera que en dicho libro se registre, adicionalmente:

a) Si las medidas constituyen una solicitud de autorización judicial previa o si se trata de una solicitud de ratificación en los casos de emergencia autorizados por la ley.

b) Identificar si la medida de intervención, acceso a datos conservados o geolocalización cuya autorización se solicita u otorga se realiza de manera autónoma o con colaboración de algún concesionario, autorizado o proveedor.

c) En su caso, identificar el concesionario, autorizado o proveedor que preste colaboración para llevar a cabo la medida de vigilancia.

d) En su caso, identificación del equipo o sistema tecnológico utilizado para llevar a cabo la medida de vigilancia de manera autónoma.

e) Identificación del número (cantidad) de personas y/o dispositivos respecto de los cuáles se solicita autorización o ratificación, para llevar a cabo la medida de vigilancia.

f) Si la solicitud de autorización o ratificación fue concedida o negada. En el caso de autorización parcial, identificar las características autorizadas o negadas que difieren de la solicitud original.

g) Identificación de la fecha de realización de actos de supervisión de las medidas autorizadas de parte de la autoridad judicial.

La información contenida en este libro debe estar estructurada de manera que la misma permita al CJF cumplir con sus obligaciones de transparencia oficiosa derivadas del artículo 70, fracción XLVII de la LGTAIP y/o responder a solicitudes de acceso a la información relacionadas con la información de carácter público que contiene dicho libro.

iv. Modificación de disposiciones administrativas por parte del IFT

Deben modificarse los "*Lineamientos de Colaboración en Materia de Seguridad y Justicia*" de manera que se reintroduzcan al Capítulo VI de los Lineamientos obligaciones de transparencia por parte de los concesionarios, autorizados y los proveedores de aplicaciones, contenidos y servicios a los que se refiere el artículo 189 de la LFTR.

Las obligaciones de transparencia de concesionarios, autorizados y proveedores contenidas en los Lineamientos deben estar homologadas con las obligaciones de las autoridades facultadas y del CJF, de manera que las mismas sean comparables. En este sentido deben adoptar una periodicidad trimestral e incluir criterios comparables.

En particular, las obligaciones de reporte estadístico por parte de concesionarios, autorizados y proveedores deben incluir, de manera desagregada:

a) Autoridad solicitante.

b) Tipo de colaboración (intervención de comunicaciones, acceso a datos conservados, localización geográfica).

c) Fundamento legal de la solicitud recibida.

d) Si la colaboración está precedida de autorización judicial o se sitúa en los casos de emergencia autorizados por la ley.

e) Número (cantidad) de personas y/o dispositivos respecto de los cuáles se solicita autorización o ratificación, para llevar a cabo la medida de vigilancia.

f) Si la solicitud fue atendida favorablemente o fue negada.

Los reportes deben ser publicados por el IFT en su portal de Internet y/o en la PNT en el menor tiempo posible posterior a su recepción por parte de los concesionarios, autorizados o proveedores.

Además es necesario asegurar que esta información sea ofrecida en un formato que permita su reutilización por los usuarios y por las máquinas, es decir, presentarse mediante el enfoque de datos abiertos, lo cual implica facilitar la posibilidad de exportar el conjunto de datos publicados en formatos estructurados para facilitar el consumo e interpretación.

V. Modificación de criterios de reserva por parte de los Comités de Transparencia de las autoridades facultadas para llevar a cabo medidas de vigilancia y por parte del INAI

I. **Información estadística.** Los comités de transparencia y los órganos garantes deben reconocer que la información estadística relacionada a las tareas de vigilancia constituyen información pública e incluso existe obligación oficiosa de publicar, por lo que deben abstenerse de considerar dicha información como reservada, inclusive cuando se refiera a investigaciones en curso.

II. **Versiones públicas de requerimientos y solicitudes de autorización o ratificación judicial.** Las autoridades facultadas para llevar a cabo medidas de vigilancia no deben reservar en su totalidad los documentos que contienen los requerimientos y solicitudes de autorización o ratificación judicial.

    Si bien es razonable testar información que identifique a los objetivos de la medida (nombres, números de teléfono, cuentas de correo) o las circunstancias de hecho específicas bajo investigación (lugares, domicilios, nombres), no debe testarse la información que permita desprender información estadística sobre las medidas de vigilancia (tipo de medida, número/cantidad de personas o dispositivos afectados, fundamento legal, alcance temporal, si la medida se lleva a cabo de manera autónoma o con colaboración de algún concesionario, autorizado o proveedor, la identidad del mismo).

III. **Versiones públicas de resoluciones respecto de solicitudes de autorización o ratificación judicial.** La autoridad judicial no debe reservar en su totalidad las resoluciones en las que autoriza, ratifica o niega las solicitudes para llevar a cabo medidas de vigilancia.

    Si bien es razonable testar información que identifique a los objetivos de la medida (nombres, números de teléfono, cuentas de correo) o las circunstancias de hecho específicas

bajo investigación (lugares, domicilios, nombres), no debe testarse la información que permita desprender información estadística sobre las medidas de vigilancia (tipo de medida, número/cantidad de personas o dispositivos afectados, fundamento legal, alcance temporal, si la medida se lleva a cabo de manera autónoma o con colaboración de algún concesionario, autorizado o proveedor, la identidad del mismo), ni testarse el contenido de la resolución que interpreta las normas que regulan las medidas de vigilancia.

IV. **Versiones públicas de documentos relacionados a la contratación de equipos y sistemas para llevar a cabo medidas de vigilancia.** Las autoridades que adquieren equipos y sistemas para llevar a cabo medidas de vigilancia no deben reservar en su totalidad la documentación relacionada a su contratación.

Es importante que cuando se solicita información respecto de estas contrataciones, las respuestas no se circunscriban únicamente al contrato y su anexo técnico, sino que existen otros documentos que forman parte del proceso de contratación que no deben omitirse.

Igualmente, es importante que no se haga el testado de información que permita conocer el monto de los contratos, la identidad de las empresas contratantes, el nombre, ni las capacidades generales de los equipos y sistemas contratados.

En este sentido, no se considera razonable testar información como el nombre comercial del equipo o sistema, ni las capacidades generales del equipo o sistema, como pueden ser las categorías de datos que pueden ser obtenidas mediante la operación del equipo o sistema o la cantidad de objetivos que pueden ser atacados, pues dicha información no permite frustrar la eficacia de los mismos, y en caso de que remotamente, en conjunto con otra información pudiera contribuir a la elusión de dichas medidas, es preponderante el interés público de la sociedad de conocer las capacidades invasivas del Estado, sobre todo en casos con indicios de abuso o la comisión de actos de corrupción.

V. **Información contenida en el registro de empresas proveedoras de equipos y sistemas, el registro de equipos y sistemas, el registro de agentes autorizados para participar en la implementación de medidas de vigilancia, el registro de uso y el registro de control judicial.**

En relación a los distintos registros que han sido propuestos. En primer lugar, es indispensable que se reconozca que toda la información contenida en dichos registros debe ser accesible para las autoridades con facultades de investigación, como la Fiscalía General de la República, así como el INAI, en el ejercicio de sus facultades.

Por otra parte, si bien se considera que parte de la información que forma parte de dichos registros puede ser legítimamente reservada respecto de su acceso por parte del público en general, se considera que en particular el registro de proveedores, así como el registro de equipos y sistemas debe considerarse, en parte, información pública. En particular, la información relacionada al nombre de las empresas registradas y el nombre comercial de los equipos y sistemas que comercializan.

I. Mecanismo extraordinario de esclarecimiento y combate a la impunidad

A partir de la absoluta impunidad en la que se encuentran los casos de vigilancia ilegal en contra de personas defensoras de derechos humanos y periodistas en México, así como de las múltiples recomendaciones internacionales sobre la necesidad de garantizar una investigación independiente e imparcial. México debe considerar establecer un mecanismo extraordinario de esclarecimiento e investigación de casos de la vigilancia ilegal.

Dicho mecanismo debe estar acompañado por organismos internacionales de protección de derechos humanos, contar con los recursos suficientes y el acceso total a los archivos gubernamentales, incluyendo los de inteligencia civil, militar y financiera, con el objetivo de esclarecer los procesos de adquisición y uso irregular de equipos y sistemas de vigilancia, así como las conductas de encubrimiento y obstrucción de justicia relacionadas.

El ESTADO DE LA VIGILANCIA

Por: Luis Fernando García Muñoz, Ana Gaitán Uribe, José Flores Sosa, Santiago Narváez Herrasti, Milan Trnka Osorio.

Ciudad de México. México, Enero 2025.

El Estado de la Vigilancia ofrece un diagnóstico de los problemas y desafíos que la vigilancia de comunicaciones representa para los derechos humanos en México y desarrolla propuestas para establecer controles democráticos que permitan prevenir, detectar y remediar el abuso de estas tecnologías.

Por más de una década, desde **R3D: Red en Defensa de los Derechos Digitales** hemos investigado y documentado evidencia de estos abusos, utilizado herramientas legales como miles de solicitudes de acceso a la información y centenares de recursos de revisión en materia de transparencia, que han resultado en el acceso de miles de documentos relevantes –reunidos y sistematizados en estas páginas– que confirman que la vigilancia en México sigue fuera de control.

A partir de los hallazgos presentados, este informe emite diversas recomendaciones para el rediseño e implementación de una reforma profunda al marco jurídico e institucional en México, de manera que las facultades de vigilancia de comunicaciones posean suficientes controles democráticos para prevenir, detectar y remediar abusos, evitar la corrupción y garantizar la verdad y justicia.