El Estado de la Vigilancia

Septiembre 2018

Hoja legal

Índice

I. Diagnóstico de la vigilancia en México: Sistemáticamente fuera de control

A. Incertidumbre jurídica sobre las facultades de vigilancia

El derecho a la privacidad se encuentra reconocido en los artículos 11 de la Convención Americana sobre Derechos Humanos (en adelante "CADH") 17 del Pacto Internacional de Derechos Civiles y Políticos (en adelante "PIDCP") y 16 de la Constitución Política de los Estados Unidos Mexicanos (en adelante "CPEUM"). La Suprema Corte de Justicia de la Nación ha determinado que el primer párrafo de este último artículo protege el derecho a la privacidad o intimidad.[1] En términos de la Corte Interamericana de Derechos Humanos (en adelante "Corte IDH") "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".[2]

Si bien el derecho a la privacidad no es un derecho absoluto; el mismo puede ser restringido únicamente cuando se garantice que las injerencias a este no sean abusivas o arbitrarias. Para ello, el derecho internacional establece los siguientes tres requisitos: i) las restricciones deben estar previstas en ley, ii) perseguir un fin legítimo y iii) cumplir con los requisitos de idoneidad, necesidad y proporcionalidad, es decir, deben ser necesarias en una sociedad democrática.[3]

En relación al primer requisito, el Tribunal Europeo de Derechos Humanos (en adelante "TEDH") determinó que atendiendo a la falta de escrutinio público y al riesgo de abuso, propios de la práctica de medidas de vigilancia secreta por parte de las autoridades públicas, la compatibilidad de esta con el estado de Derecho requiere que las leyes nacionales prevean garantías efectivas y adecuadas en contra de interferencias arbitrarias al derecho a la vida privada.[4]

---

[1] Véase por ejemplo, Tesis: 2ª. LXIII/2008, Novena Época, 2ª Sala, Semanario Judicial de la Federación y su Gaceta, Tomo XXVII, Mayo de 2008, página 229. Rubro: DERECHO A LA PRIVACIDAD O INTIMIDAD. ESTÁ PROTEGIDO POR EL ARTÍCULO 16, PRIMER PÁRRAFO, DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS.

[2] 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; *Caso Escher y otros vs. Brasil*. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 6 de julio de 2009. Serie C No. 200, párr. 113; y *Caso Fernández Ortega y otros vs. México*. Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia de 30 de agosto de 2010. Serie C No. 215, párr. 157.

[3] CoIDH. *Caso Tristán Donoso vs. Panamá*. Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia de 27 de enero de 2009. Serie C No. 193, párr. 56.

[4] TEDH. Uzun v. Germany, párr. 63

En ese sentido, en la Declaración Conjunta sobre Programas de Vigilancia y su impacto en la Libertad de Expresión de los Relatores Especiales para la Libertad de Expresión de la ONU y la Comisión Interamericana de Derechos Humanos[5], se contempla que las leyes sobre intervención, recolección y uso de información personal deberán 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.

Por tanto, la ley debe ser lo suficientemente clara en sus términos para otorgar a los ciudadanos una indicación adecuada respecto de las condiciones y circunstancias en que las autoridades están facultadas para recurrir a dichas medidas.[6] Además, las medidas deben basarse en una ley que sea particularmente precisa sobre todo si se toma en cuenta que la tecnología disponible para realizar esas actividades continuamente se vuelve más sofisticada.[7] Bajo este orden de ideas, la legislación en materia de vigilancia debe establecer de manera clara, precisa y detalla aspectos fundamentales como:

1. Las autoridades expresamente facultadas para llevar a cabo la medida;
2. La definición de la categoría de personas que pueden ser afectadas;
3. La duración del plazo en la que puede ser llevada a cabo la medida:
4. El procedimiento que debe seguirse para el tratamiento, almacenamiento, transmisión y destrucción de los datos obtenidos mediante la medida:
5. El grado de relación que debe existir entre la persona que será afectada por la medida y los datos que permitan sugerir que se encuentra relacionada con la comisión de un hecho delictivo para que la medida pueda llevarse a cabo.

Además de lo anterior, de conformidad con los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones (en adelante “los Principios”) la legislación debe establecer como requisito para llevar a cabo medidas de vigilancia que estas sean previamente autorizadas por una autoridad judicial competente, imparcial e independiente[8].

A lo largo de los apartados siguientes se analizará si la actual legislación mexicana en materia de vigilancia cumple con los estándares internacionales anteriormente referidos.

1. ¿Quiénes pueden vigilar?

[5] 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 para la Libertad de Expresión. Disponible en: https://www.oas.org/es/cidh/expresion/ showarticle.asp?artID=926&IID=2

[6] 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.

[7] TEDH. *Uzun vs. Alemania*, párr. 61; *Weber y Saravia vs. Alemania*, párr. 93.

[8] Principio 6 de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponibles en: https://necessaryandproportionate.org/principles

En México, en primer lugar, la Constitución le reconoce facultades para ejercer funciones de vigilancia a: las (i) autoridades federales facultadas por una ley y (ii) el titular del Ministerio Público de las entidades federativas[9]. Ahora bien, las leyes que hasta el momento prevén o regulan tareas de vigilancia son: artículos 291 y 303 del Código Nacional de Procedimientos Penales (CNPP); artículo 11 Bis 1 de la Ley Federal Contra la Delincuencia Organizada (LFCDO); artículos 189 y 190 fracciones I, II y III de la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR); artículo 24 de la Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro (LGPSDMS); artículo 8 fracciones XXVIII y XXIX de la Ley de la Policía Federal (LPF); artículos 29 y 30 de la Ley de Seguridad Interior (LSI), artículo 34 de la Ley de Seguridad Nacional (LSN) y los Lineamientos de Colaboración en materia de Seguridad y Justicia (Lineamientos de Colaboración).

Una vez identificado el catálogo de leyes que contemplan medidas de vigilancia, resulta necesario analizar si cada una de ellas aclara o no las autoridades que conforme a estas están facultadas para llevar a cabo tareas de vigilancia:

El CNPP en su artículo 303 establece que será el Procurador o el servidor público en quien se delegue la facultad quienes podrán solicitar al Juez de control que requiera a los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos su colaboración en materia de localización geográfica en tiempo real y solicitud de entrega de datos conservados.

Para el caso de la LFCDO, en su artículo 16, también se reconoce que la autoridad facultada para realizar las solicitudes de intervención de comunicaciones al Juez Federal de control será el Titular de la Procuraduría General de la República o los servidores públicos en quienes se delegue la facultad.

En lo que respecta a la LFTR, esta prevé en sus artículos 189 y 190, fracciones I y III, que los concesionarios de telecomunicaciones y en su caso, los autorizados o proveedores de servicios de aplicaciones y contenidos, deberán colaborar con las “autoridades competentes en los términos que establezcan las leyes” cuando éstas les requieran la localización geográfica, en tiempo real, de los equipos de comunicación móvil así como los registros y control de comunicaciones de sus usuarios, señalando que “serán las instancias de seguridad y procuración de justicia quienes designarán a los servidores públicos encargados de gestionar los requerimientos que se realicen a los concesionarios".

De lo anterior resulta claro que el legislador no contempló especificar dentro de la misma ley quiénes son las autoridades competentes para ejercer las facultades en cuestión, limitándose a remitir a "las leyes” sin mayor especificación o aclaración al respecto; mientras que en los Lineamientos de Colaboración de la propia ley tampoco se prevé expresamente quiénes son las autoridades con dichas facultades.

Mientras que la LGPSDMS no es tan clara al respecto de las autoridades encargadas de realizar actividades de vigilancia en la materia pues únicamente se limita a señalar en su

[9] Artículo 16, párrafo decimosegundo

artículo 24 que para la intervención y aportación voluntaria de comunicaciones privadas, se estará a lo dispuesto en el Código Nacional.

Por su parte, la Ley de la Policía Federal en su artículo 8 fracción XXVIII señala como una de las atribuciones de la policía federal el solicitar por escrito, previa autorización del Juez de control a los concesionarios, permisionarios, operadoras telefónicas y todas aquellas comercializadoras de servicios en materia de telecomunicaciones, de sistemas de comunicación vía satélite, la información con que cuenten, así como georreferenciación de los equipos de comunicación móvil en tiempo real, para el cumplimiento de sus fines de prevención de los delitos.

La LSI prevé en su artículo 30 de forma bastante amplia y ambigua que serán las Fuerzas Federales y las Fuerzas Armadas quienes desarrollarán actividades de inteligencia, mientras que en la LSN su artículo 19 fracción I, establece que las actividades de inteligencia son parte de las operaciones del Centro de Investigación y Seguridad Nacional (CISEN).

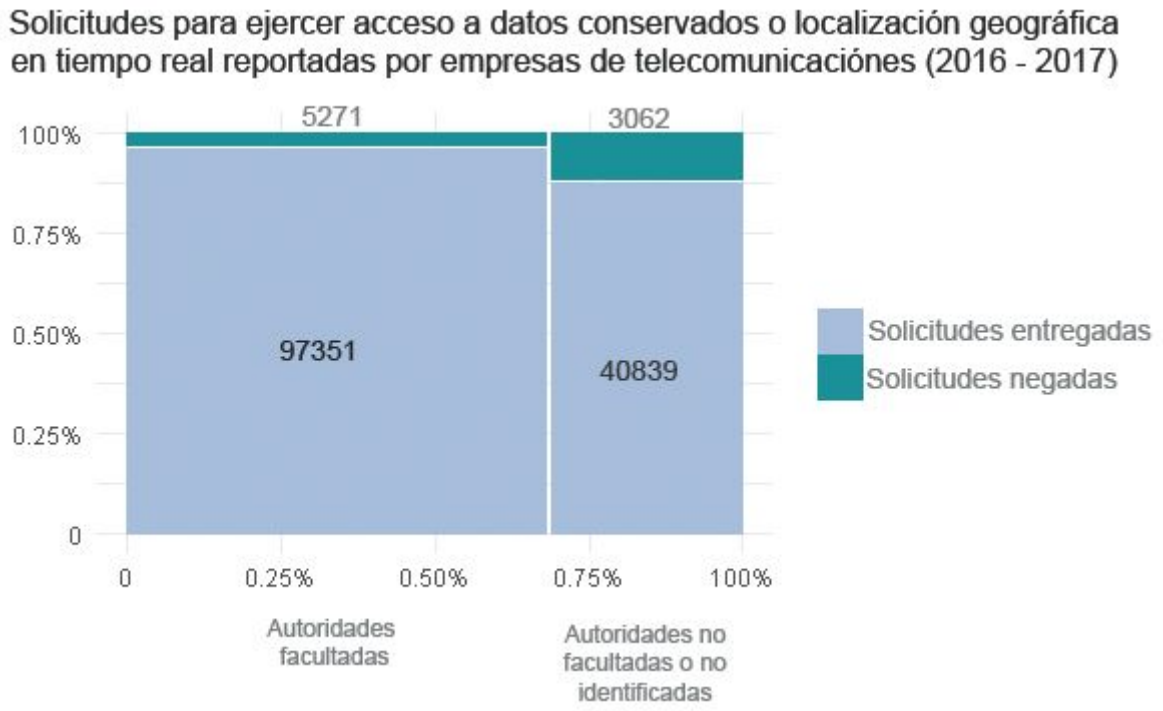
No obstante sería posible desprender de los párrafos anteriores un catálogo de autoridades facultadas para llevar a cabo funciones de vigilancia y requerir la colaboración de las concesionarias, autorizadas o proveedores en este sentido, R3D ha documentado que estas últimas han proporcionado la localización geográfica y los metadatos de comunicaciones de sus usuarios a autoridades que NO están facultadas para requerirlos o sin que medie la autorización judicial necesaria para ello.

Incluso, ante la falta de claridad respecto de las autoridades facultadas para ejercer vigilancia específicamente en lo que concierne a la LFTR, R3D presentó un amparo que acabó siendo atraído por la SCJN, bajo el expediente AR 964/2015. Derivado de dicho amparo, la SCJN estableció que únicamente el Centro Nacional de Investigación y Seguridad Nacional (CISEN), la Policía Federal, el titular de la Procuraduría General de la República (PGR) están facultados para llevar a cabo las herramientas de vigilancia encubierta previstas por la misma LFTR. No obstante, aun en aplicación de esta ley R3D ha documentado que se han cumplimentado requerimientos de los metadatos de comunicaciones previstos por la LFTR para autoridades que no están expresamente facultadas para solicitarlos.

Todo lo anterior evidencia que en México tanto en el sector público como en el privado cuentan con incertidumbre sobre qué autoridades son las que tienen facultades para ejercer vigilancia y los ejercicios abusivos en este sentido persisten.

De los informes remitidos al IFT, se desprende que entre el año 2016 y el 2017 alrededor del 30 por ciento de las 146, 523 solicitudes en las que se pidió el acceso a datos conservados (ADC) o la localización geográfica en tiempo real (LGTR) de usuarios de telecomunicaciones fueron realizadas por autoridades no identificadas o que no cuentan con la facultad para ejercer vigilancia, como las secretarías de Marina y de Hacienda, los Gobiernos del Estado de Colima, del Estado de México, los institutos electorales del estado de Oaxaca y de la Ciudad de México, entre otras. En el 88% de dichas solicitudes,

realizadas por autoridades no facultadas o no identificadas, los concesionarios y autorizados de telecomunicaciones entregaron la información, vulnerando los derechos de miles de sus usuarios y en desobediencia a lo clarificado por la Suprema Corte de Justicia de la Nación.



Gráfica 1. Fuente: realización propia con datos de los informes remitidos al IFT por empresas de telecomunicaciones en 2016 y 2017.

No conforme la anteriormente evidenciada falta de claridad respecto de qué autoridades pueden llevar a cabo funciones de vigilancia en la práctica, recientemente el Tribunal Electoral del Poder Judicial de la Federación[10] (TEPJF) resolvió, en la sentencia SUP-RAP-193/2018 y acumulados, que la Unidad Técnica de lo Contencioso Electoral de la Secretaría Ejecutiva del Instituto Nacional Electoral (INE) tiene la facultad de requerir que se le compartan datos personales (nombre y domicilio) de las y los titulares de ciertas líneas telefónicas bajo el argumento de que dichos datos no tienen relación alguna con el contenido o datos de tráfico de un proceso comunicativo en específico y por tanto, no se encuentran protegidos por la garantía constitucional del derecho a la privacidad regulado por el artículo 16 constitucional.

Lo anterior es incompatible con n el artículo 190 de la LFTR ya que este claramente enlista como parte de los metadatos de comunicaciones que deben ser conservados por las empresas de telecomunicaciones para colaborar con a las autoridades facultadas en

[10] TEPJ. EXPEDIENTES: SUP-RAP-193/2018 Y ACUMULADOS. Sentencia del 25 de julio de 2018. Disponible en: http://www.te.gob.mx/Informacion_juridiccional/sesion_publica/ejecutoria/sentencias/SUP-RAP-0193-2018.pdf

materia de seguridad y procuración de justicia, entre las cuales naturalmente no se encuentra el INE. En este sentido, la resolución del TEPJF es además inconstitucional considerando que el mismo artículo 16 constitucional expresamente establece que cualquier injerencia a las comunicaciones privadas está prohibida en materia electoral, fiscal, mercantil, civil, laboral o administrativo.

2. ¿Cuándo y cómo pueden vigilar?

De igual forma, las leyes anteriormente referidas tampoco especifican de manera clara, precisa y detallada los motivos o circunstancias por los cuales las autoridades facultadas pueden llevar a cabo funciones de vigilancia.

Para empezar, el CNPP le concede al ministerio público la facultad de solicitar r la localización geográfica en tiempo real o entrega de datos conservados de cualquier persona siempre que este "lo considere necesario", sin especificar mayor requerimiento, limitación o consideración al respecto.

De manera preocupante, tanto la LGPSDMS como la LSN, remiten a este código de forma supletoria para regular la práctica de intervención de comunicaciones que derive de su aplicación.

Por su parte, en la LFCDO tampoco se prevé como requisito mínimo para poder llevar a cabo funciones de vigilancia que existan indicios claros de que se ha cometido alguno de los delitos contemplados en la misma ley.

Dada la vaguedad de la LFTR, la SCJN tuvo que intervenir y especificar la necesidad de que exista previa autorización judicial para el acceso a datos conservados conforme a la misma[11].

En lo que respecta a la LPF, esta es la única que contempla la necesidad de que existan *indicios suficientes que acrediten que se está organizando la comisión de los delitos* previstos en ella; no obstante, la misma contempla un catálogo por demás extenso de delitos para los cuales es posible realizar actividades de vigilancia. No conforme, esta no ahonda en qué se deberá entender como "indicios suficientes" para poder ejercer dichas actividades.

Por el otro lado, la LSI ni siquiera contempla, para poder llevar a cabo labores de vigilancia, que deba mediar la autorización judicial correspondiente. La misma simplemente se limita a establecer que los sujetos regulados por esta están facultados para desarrollar *"actividades de inteligencia en los ámbitos de sus respectivas competencias".*

La vaguedad de las leyes que regulan las funciones de vigilancia estatales que han sido analizadas denota que la legislación mexicana dista de cumplir con el requisito mínimo de que dichas funciones estén condicionadas a la existencia de indicios claros de la comisión

[11] SCJN. Segunda Sala. Amparo en Revisión 964/2015. Sentencia del 2015.

de un delito. Consecuentemente, las mismas fomentan el ejercicio de actividades de vigilancia de manera arbitraria y discrecional, siendo prácticamente imposible analizar si estas se adhieren a los estándares internacionales de necesidad y proporcionalidad para cumplir con un fin que efectivamente sea legítimo en cualquier Estado de derecho.

Las diferentes formas en que se pueden llevar a cabo las actividades de vigilancia pueden afectar de forma distinta la vida privada de las personas por lo que debe existir un tratamiento diferenciado.

A continuación se enlistan los diferentes tipos de actividades de vigilancia previstos por la legislación mexicana:

CNPP	1. Intervención de comunicaciones; 2. Extracción de información; 3. Localización geográfica; 4. Acceso a datos conservados.
LFCDO	1. Recabar información en lugares públicos, mediante la utilización de medios e instrumentos y cualquier herramienta que resulten necesarias para la generación de inteligencia; 2. Vigilancia electrónica; 3. Intervención de comunicaciones; 4. Extracción de información; 5. Localización geográfica; 6. Acceso a datos conservados.
LFTR	1. Acceso a datos conservados; 2. Localización geográfica en tiempo real.
LGPSDMS	1. Intervención de comunicaciones conforme lo dispuesto en el CNPP; 2. Proponer la celebración de convenios con las empresas de telecomunicaciones para la obtención de datos adicionales contenidos en la base de datos prevista en la LFTR y sobre el uso de las mismas.
LPF	1. Acceso a datos conservados 2. Localización geográfica en tiempo real 3. Intervención de comunicaciones
LSI	1. Actividades de inteligencia
LSN	1. Intervención de comunicaciones

- La reserva de versiones públicas de solicitudes para ejercer vigilancia, resoluciones relativas a éstas mantienen ambigüedad sobre cuándo y cómo se utilizan medidas de vigilancia.

Además de lo enunciado en los párrafos anteriores, el hecho de que las leyes sobre el ejercicio de la vigilancia sean ambiguas provoca que la forma en que se apliquen dependa fuertemente de la interpretación que el poder judicial les da. Por ello se puede decir que en cierta forma, conocer la forma en que se interpretan dichas leyes equivale a conocer realmente las medidas de vigilancia.

En este sentido R3D ha realizado aproximadamente 110 solicitudes de acceso a la información para obtener las versiones públicas de las resoluciones del poder judicial a los pedimentos de las autoridades para ejercer vigilancia. Sin embargo en cerca del 60 por ciento de dichas solicitudes las autoridades respondieron reservando las versiones públicas, alegando que la divulgación de dicha información atenta en contra de las facultades de vigilancia y de las investigaciones en proceso. Adicionalmente en alrededor del 26 por ciento de dichas solicitudes las autoridades no contestaron a lo solicitado.

La reserva de dicha información pública le da, de facto, un carácter de secrecía a las leyes de vigilancia en el país e imposibilita conocer las capacidades de vigilancia con las que cuenta el Estado mexicano y la forma en que las ejerce.

Por otra parte, es argumentable que el hecho de que en la práctica las facultades de vigilancia estén definidas mayoritariamente a partir de la interpretación que el poder judicial da a las leyes y no a partir de las leyes en la materia -debido a que las mismas son poco claras- le resta parte del valor democrático que estas leyes pudieran tener, al no ser producto de un debate público, sino de la interpretación que el sistema judicial les da.

B. Proliferación en el uso de herramientas de vigilancia ilegales e invasivas

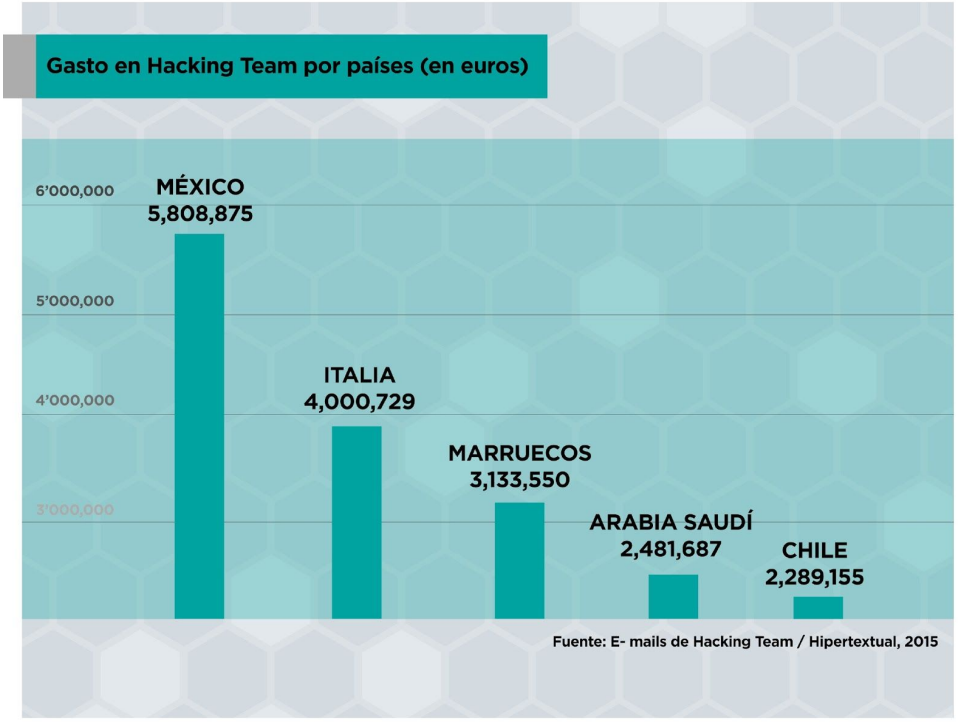
En los últimos años, se ha revelado que numerosas autoridades mexicanas han adquirido y utilizado tecnologías altamente sofisticadas de vigilancia. En particular, existe evidencia de que diversas autoridades, tanto federales como estatales, cuentan con la capacidad de infectar computadoras y teléfonos móviles con distintos tipos de software malicioso, que les permite extraer información de los dispositivos e incluso tomar control de estos para ejercer una vigilancia focalizada total.

La utilización de esta forma de vigilancia en México es sumamente problemática por varias razones. En primer lugar, porque otorga un poder invasivo sumamente amplio, el cual difícilmente puede justificarse a la luz de los principios de necesidad y proporcionalidad.

Así mismo, la infección de dispositivos con software de vigilancia ocurre usualmente como consecuencia de la explotación de vulnerabilidades en redes, sistemas y dispositivos que suele no ser conocidas por los proveedores o fabricantes, poniendo en riesgo la privacidad y seguridad de todos los usuarios de esos servicios.

Malware de Estado: un gasto desmedido

La adquisición de herramientas sofisticadas de vigilancia representa un gasto desproporcionado e injustificado de dinero público. De acuerdo con la filtración de correos electrónicos y documentos internos de la firma italiana Hacking Team, revelados el 5 de julio de 2015[12], se mostró que dicha empresa de software de espionaje había vendido sus productos a gobiernos de países bajo graves crisis de derechos humanos, tales como Bahréin, Sudán o Uzbekistán. De un total de 35 naciones, **México resultó ser el principal cliente de la firma**, con transacciones hechas por parte de diferentes gobiernos locales, dependencias y agencias federales a través de empresas intermediarias[13] 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.



[12] Privacy International (6 de julio de 2015) Surveillance company Hacking Team exposed. Disponible en: https://www.privacyinternational.org/node/618

[13] Angel, A. (7 de julio de 2015) México, el principal cliente de una empresa que vende software para espiar. *Animal Político*. 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/

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).

Tabla 2. Clientes estatales de Hacking Team en México

Cliente	**Intermediarios**	**Negociación**	**Compra**	**Identificador**	**Gasto aproximado**
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	210,000 euros (estimado de acuerdo a cotización)
Gobierno de Campeche	Grupo Kabat / SYM Servicios Integrales		Entregado en mayo de 2013. Pago por 386 mil euros.	SDUC	386,296 euros (facturado por 2013-2014)
Gobierno de Chiapas	Servicios Integrales Heres	Solicitud de reunión en junio de 2015.	No se sabe.	No.	No hubo.
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	550 mil euros (cotización)
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	265 mil euros (facturado en 2014)
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	255 mil euros (2012) 250 mil euros (2013)
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	

C. Control judicial inexistente o simulado

Como fue mencionado anteriormente, el ejercicio de funciones de vigilancia debe cumplir con el requisito previo de que exista la autorización judicial correspondiente, misma que deberá demostrar se cumple cuando menos con los siguientes criterios:

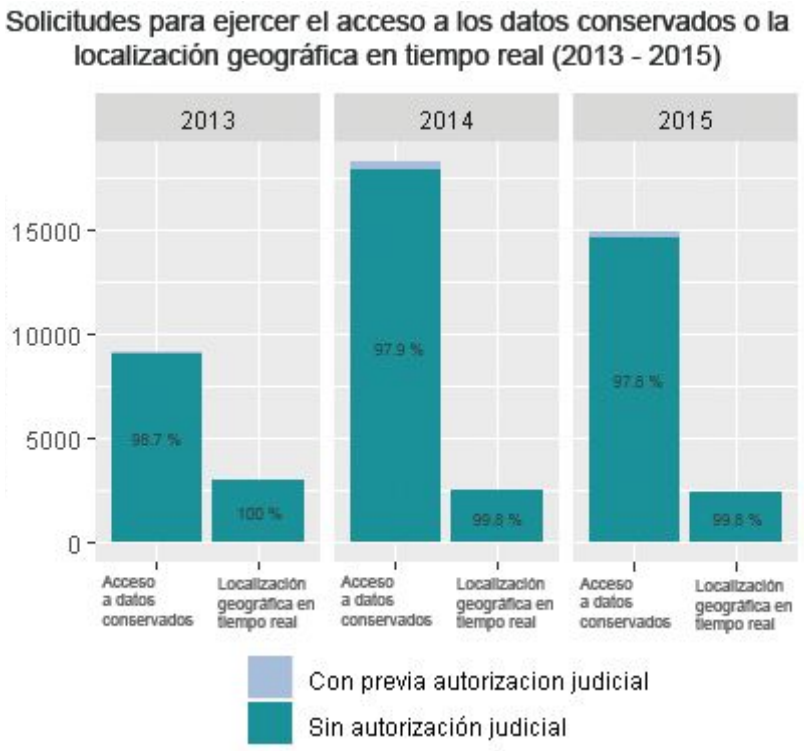
1. Es altamente probable que se haya cometido, o vaya a cometerse, un delito grave o una amenaza específica para un fin legítimo;
2. Es altamente probable que las evidencias pertinentes y materiales de un delito tan grave o amenaza específica para un fin legítimo se conseguirían mediante la medida en cuestión;
3. Se han agotado otras técnicas de investigación que son menos invasivas o estas serían inútiles, siendo la medida en cuestión la menos invasiva en la práctica;
4. La información a la que se accederá estará limitada a lo relevante y material para el delito grave o la amenaza específica al fin legítimo alegado;
5. No se recabará cualquier información que vaya más allá del fin legítimo buscado, siendo en su lugar destruida o devuelta con prontitud;
6. La información será accesada únicamente bajo los términos para los cuales fue autorizada (autoridad competente, objetivo y duración) y
7. Que como resultado de la medida no se menoscabe la esencia del derecho a la privacidad.

La única excepción aplicable al requisito de autorización judicial previa corresponde a las situaciones de emergencia, en las que existe un riesgo inminente contra la vida o la libertad de las personas. Aun en dichos casos, se debe obtener una autorización posterior, con efecto retroactivo y durante un plazo razonable y factible. Cabe mencionar que de conformidad con los Principios, el mero riesgo de fuga o de destrucción de pruebas no es suficiente para justificar la procedencia de esta excepción.

1. Datos sobre solicitudes realizadas mediante autorización judicial / sin autorización judicial.

Ahora bien, en México el requisito de autorización judicial previa para la intervención de comunicaciones se encuentra expresamente previsto por el el artículo 16 constitucional . No obstante, el surgimiento de nuevas formas de vigilar, relativas a la retención masiva de datos de usuarios de telecomunicaciones, servicios y aplicaciones de Internet derivado de la LFTR vino acompañado de incertidumbre jurídica respecto de si estas requerían de previa autorización judicial debido a la vaguedad y falta de claridad de la misma en este sentido.

Como prueba de ello, R3D documentó que más del 90 por ciento de las veces en que una autoridad tuvo acceso a los datos conservados o a la localización geográfica en tiempo real de las y los usuarios de telecomunicaciones, entre los años 2013 y 2015, lo hizo sin la autorización judicial correspondiente.



Gráfica 2. Fuente: realización propia con datos obtenidos mediante solicitudes de acceso a la información.

Incluso, de manera preocupante, entre 2013 y 2015 todas la autoridades consideradas en el presente estudio -excepto la Fiscalía General de Quintana Roo- realizaron la localización geográfica en tiempo real sin previa autorización judicial. En el caso del acceso a datos conservados cerca del cuarenta por ciento de las autoridades realizaron entre el 80 y el 100 por ciento de sus solicitudes sin previa autorización judicial.

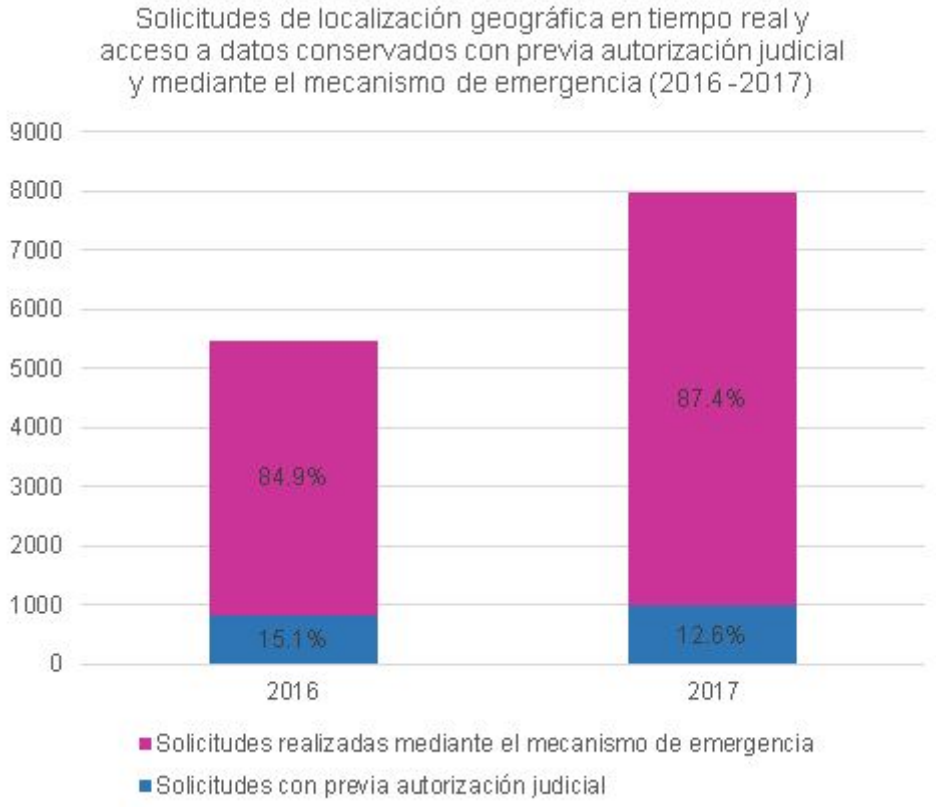
En el mismo periodo resaltan además los ejemplos de las Fiscalías de Chihuahua y Veracruz, quienes realizaron el cien por ciento de sus solicitudes para ejercer vigilancia sin contar con autorización judicial previa. Cabe mencionar que las solicitudes de estas dos autoridades representan cerca del 20 por ciento del total de solicitudes de vigilancia realizadas entre los años 2013 y 2015 reportadas por autoridades con facultades de vigilancia.

En función de lo anterior, como resultado del amparo interpuesto por R3D mencionado previamente, mediante una interpretación del artículo 16 constitucional junto con el artículo 11 de la CADH, la SCJN concluyó que no sólamente la intervención de comunicaciones, sino el acceso a datos y metadatos de las comunicaciones debe de contar con previa autorización judicial.

2. Datos sobre uso y abuso de mecanismos de emergencia.

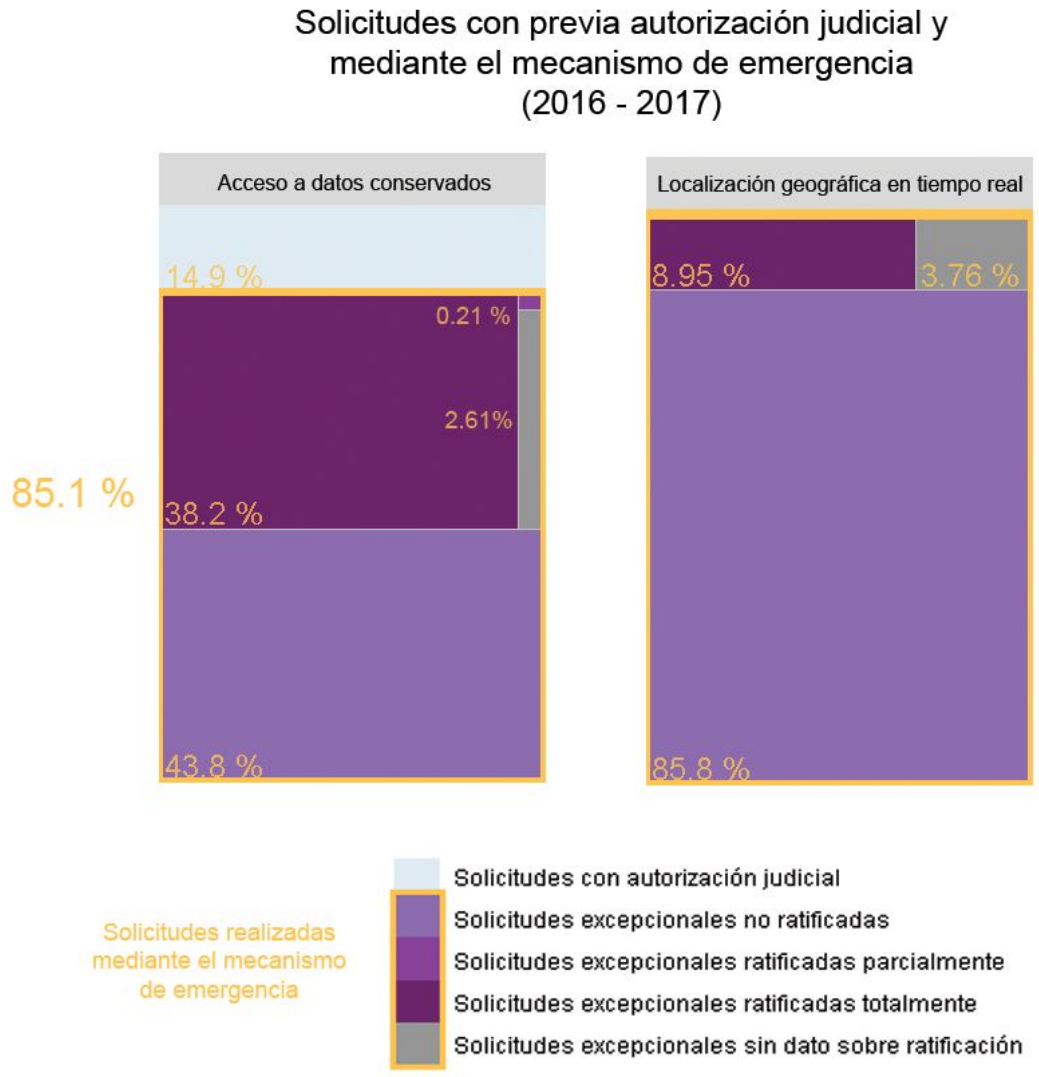
En lo que concierne a tareas de vigilancia para situaciones de emergencia, en México la única ley que regula tal excepción es el CNPP. Este, en su artículo 303, establece que no será necesaria la previa autorización judicial en casos excepcionales en los que la vida o

integridad de la víctima esté en peligro, agregando que en dichos casos se deberá solicitar la autorización judicial correspondiente en un plazo que no podrá exceder las 48 horas siguientes al momento en que se ejerció la vigilancia. Ahora bien, no obstante dicha medida es, como ya se mencionó, excepcional, entre los años 2016 y 2017 la misma se utilizó en más del 85 por ciento de los casos en que se solicitó el acceso a datos conservados o la localización geográfica en tiempo real, como lo muestra la gráfica siguiente.



Gráfica 3. Fuente: realización propia con datos obtenidos mediante solicitudes de acceso a la información.

No conforme, en cerca del 60 por ciento de los casos anteriores la medida en cuestión no fue ratificada o fue ratificada de manera parcial. Tomando en cuenta el porcentaje de solicitudes realizadas mediante el mecanismo de emergencia y el porcentaje de las mismas que no fueron ratificadas se puede concluir que en más de la mitad de las solicitudes de localización geográfica en tiempo real y acceso a datos conservados realizadas entre 2016 y 2017 se ejerció vigilancia de manera injustificada.



Gráfica 4. Fuente: realización propia con datos obtenidos mediante solicitudes de acceso a la información.

En este sentido, sobresale el caso de la Fiscalía General de Jalisco, la cual hizo uso del mecanismo de emergencia en el 99 por ciento de sus 2779 solicitudes de acceso a datos conservados y localización geográfica en tiempo real entre 2016 y 2017. De ese total de solicitudes además, el 91 por ciento no fue ratificada por la autoridad judicial competente. También está el ejemplo de la Procuraduría General de Justicia del Estado de Durango, la cual realizó el 100 por ciento de sus 609 solicitudes de ADC y LGTR mediante el mecanismo de emergencia. Peor aún, ninguna de ellas obtuvo la ratificación correspondiente.

Gráfica 5. Fuente: realización propia con datos obtenidos mediante solicitudes de acceso a la información.

La práctica generalizada de abuso del mecanismo de emergencia plantea importantes dudas sobre las motivaciones que llevaron al ejercicio de vigilancia, el uso y destino de los datos obtenidos, así como sobre la reparación en caso de que hubiese existido alguna vulneración de derechos.

En función de todo lo anterior es dable concluir que la legislación mexicana no contempla salvaguardas adecuadas y suficientes en contra del abuso de medidas de vigilancia secreta. Además de no establecerse explícitamente el control judicial previo para todas las medidas de vigilancia y de no definir con absoluta claridad y certeza la naturaleza, alcance y duración de las mismas así como las autoridades facultadas para llevarlas a cabo, el procedimiento a seguir y bajo qué supuestos, la legislación tampoco contempla salvaguardas como la supervisión independiente o el derecho de notificación al afectado. Lo anterior impide analizar si la ejecución de herramientas de vigilancia por las autoridades estatales se adhiere a los estándares internacionales de necesidad, proporcionalidad e idoneidad, obstaculizando por tanto la detección, investigación y sanción de prácticas abusivas en este sentido.

D. Opacidad de la vigilancia

1. Incumplimiento de obligaciones de transparencia

La transparencia es otra de las medidas de control democrático al ejercicio de la vigilancia que puede aportar a la rendición de cuentas así como a la sanción de su abuso. A partir del año 2014 se incluyó en la legislación mexicana obligaciones de transparencia en materia de prácticas de vigilancia tanto para autoridades como para empresas. Lamentable, hasta ahora, dichas medidas han estado lejos de fungir como un control efectivo a la vigilancia.

Tal es el caso de la obligación inscrita en el artículo 70, sección XVLII de la Ley General de Transparencia y Acceso a la Información Pública (LTAIP), la cual manda a las autoridades facultades a publicar de manera trimestral información sobre el ejercicio de la vigilancia[14].

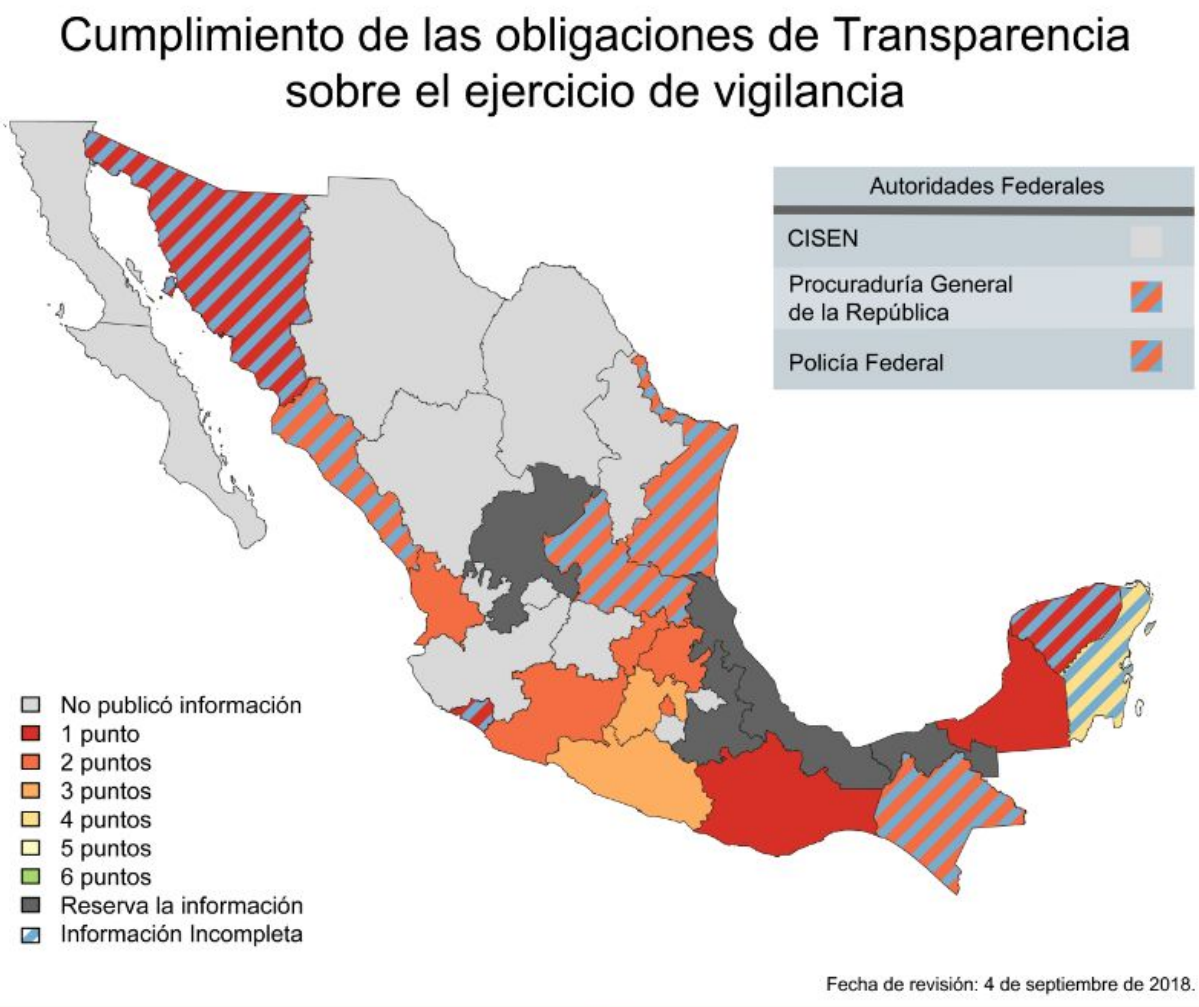
A partir de la medición de 4 criterios[15] se observó que hasta el 4 de septiembre de 2018 ninguna de las 3 autoridades federales y de las 32 autoridades locales con facultades de vigilancia habían cumplido plenamente con dichas obligaciones, del tercer trimestre de 2015 al segundo trimestre de 2018. Doce de las 35 autoridades, no publicaron información alguna en la Plataforma Nacional de Transparencia o en sus sitios. Las autoridades que publicaron alguna información lo hicieron de manera desactualizada, o inconsistente[16], sin seguir los formatos establecidos por ley, o inclusive hay casos en los que declararon la información -pública por ley- como reservada. Debido a dichas irregularidades la información que se desprende del (in)cumplimiento de dicha obligación representa un ejercicio inútil de rendición de cuentas.

El siguiente mapa muestra la puntuación del cumplimiento de los criterios que obtuvieron las autoridades federales y locales. El cumplimiento de los criterios 1 a 3 otorga un máximo de 6 puntos (un punto si la información publicada en la Plataforma Nacional de Transparencia cumple con el criterio y un punto si la información publicada en el sitio de la autoridad cumple). El incumplimiento del cuarto criterio está representado por las categorías de información reservada y la de publicación de información incompleta.

[14] Según el artículo 70, SECCIÓN XLVII de la LGTAIP las autoridades con facultades de vigilancia tienen que publicar " 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,"

[15] Los primeros 3 criterios para evaluar el cumplimiento de las obligaciones fueron construidos a partir de los artículos 60, 62 de la LTAIP, así como también de los Lineamientos Técnicos Generales de dicha Ley, dichos criterios son los siguientes: 1. La información está publicada en la Plataforma Nacional de Transparencia y en el sitio de la autoridad, 2.La información pública está actualizada (hasta el trimestre cumplido más reciente) y 3. La información publicada cumple con el formato establecido en la LGTAIP y en los lineamientos técnicos de dicha ley. El último criterio se refiere a otras irregularidades como por ejemplo la reserva de la información publicada, la publicación de información incompleta o que no guarda relación con la obligación.

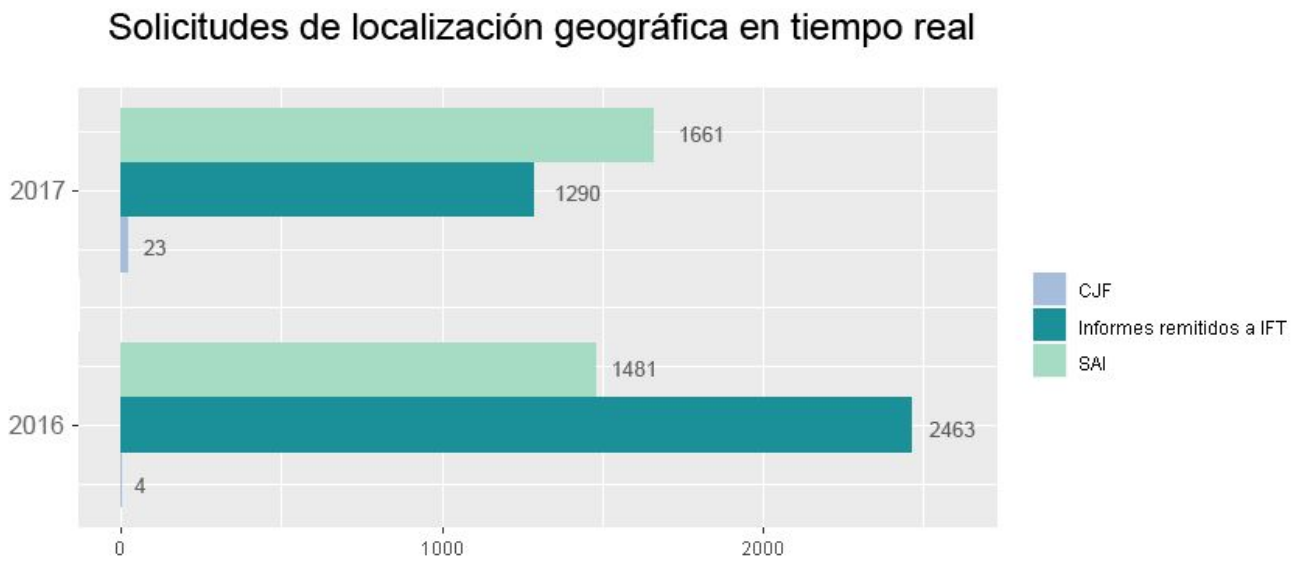
[16] Existen inconsistencias internas en la información publicada y con la información obtenida mediante el acceso a la información, lo cual plantea dudas sobre la veracidad de la información otorgada por las autoridades. Entre estos casos se encuentra lo publicado por el Centro de Investigación y Seguridad Nacional, por las fiscalías generales de los Estados de Yucatán, Quintana Roo, la Procuraduría General de Justicia de Tamaulipas, entre otras.



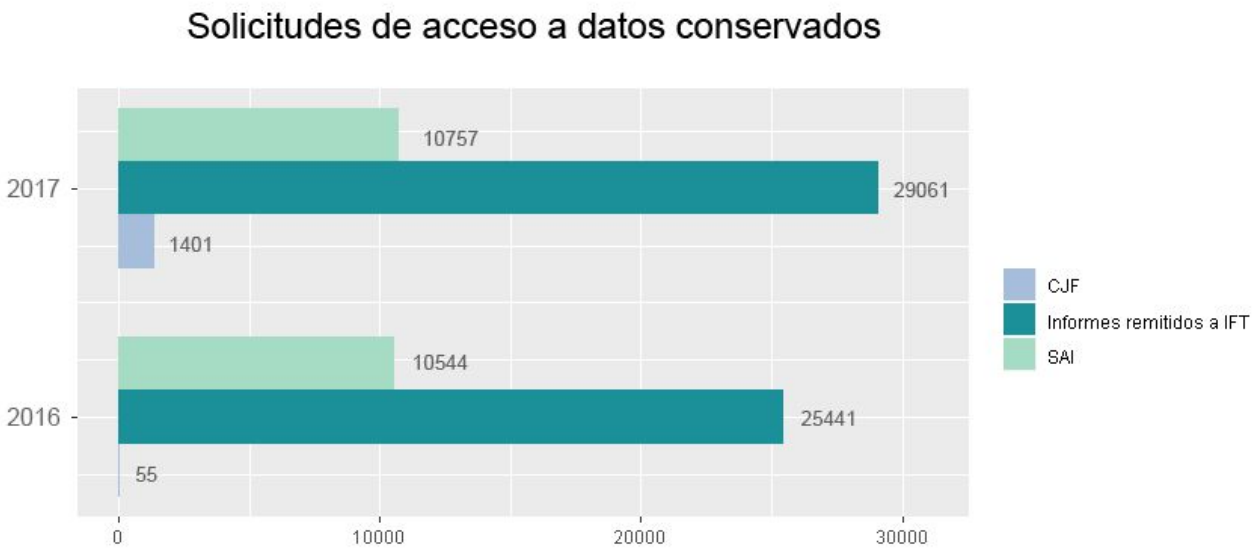
Fuente: Plataforma Nacional de Transparencia.

2. Inconsistencias entre números reportados por distintas fuentes sobre el ejercicio de vigilancia

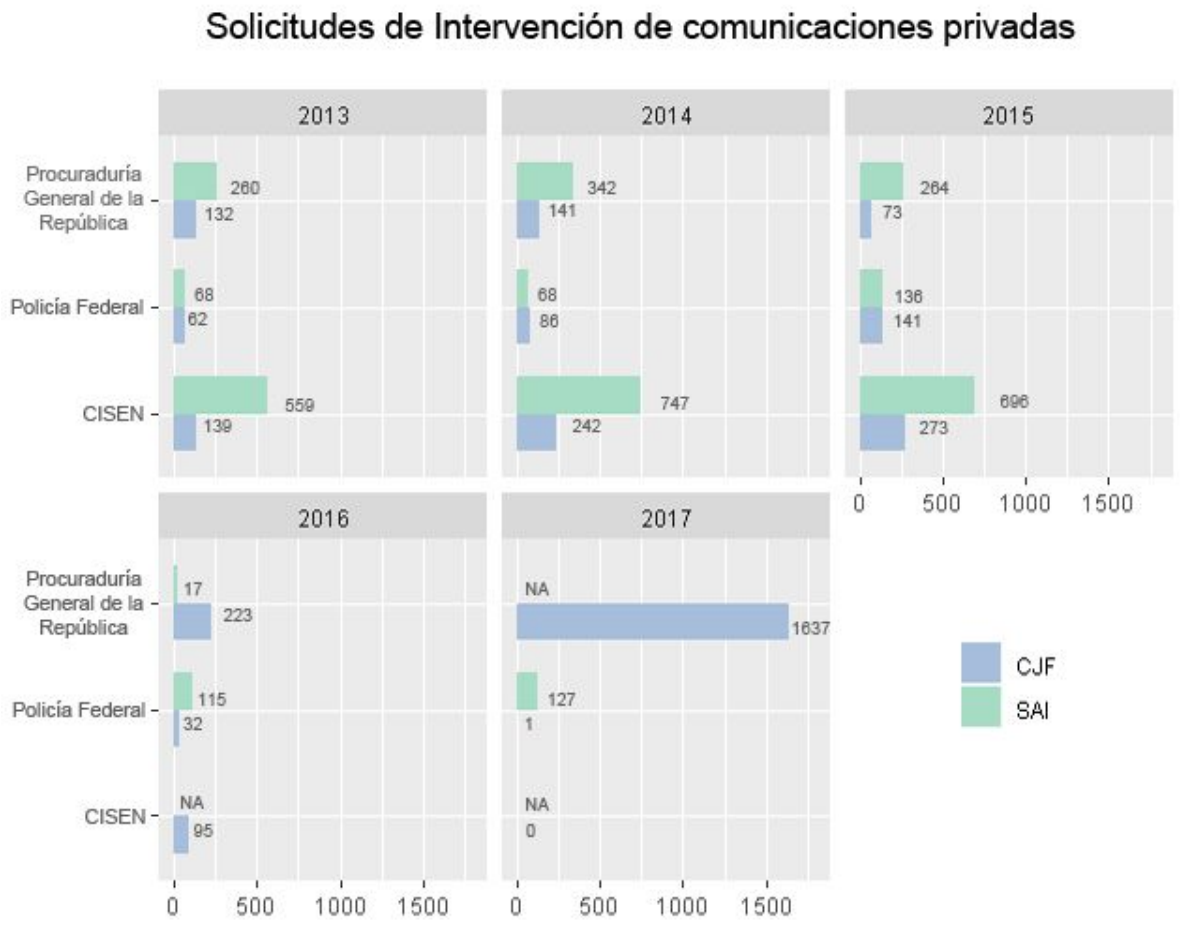
Además de la indisponibilidad de la información otra carencia con la que cuenta la transparencia en materia de vigilancia actualmente es la falta de consistencia que existe entre la información reportada por distintas las fuentes: autoridades con facultades de vigilancia, autoridades del poder judicial y empresas de telecomunicaciones. Las gráficas siguientes están compuestas por información obtenida mediante solicitudes de acceso a la información dirigidas a las autoridades con facultades de vigilancia, a la autoridad judicial, a partir de la publicación de información relativa a las obligaciones de transparencia en materia de vigilancia y mediante los datos reportados por las empresas de telecomunicaciones al Instituto Federal de Telecomunicaciones (IFT) muestran la gran inconsistencia que existe entre datos que hablan de lo mismo, las veces que se ha vigilado.



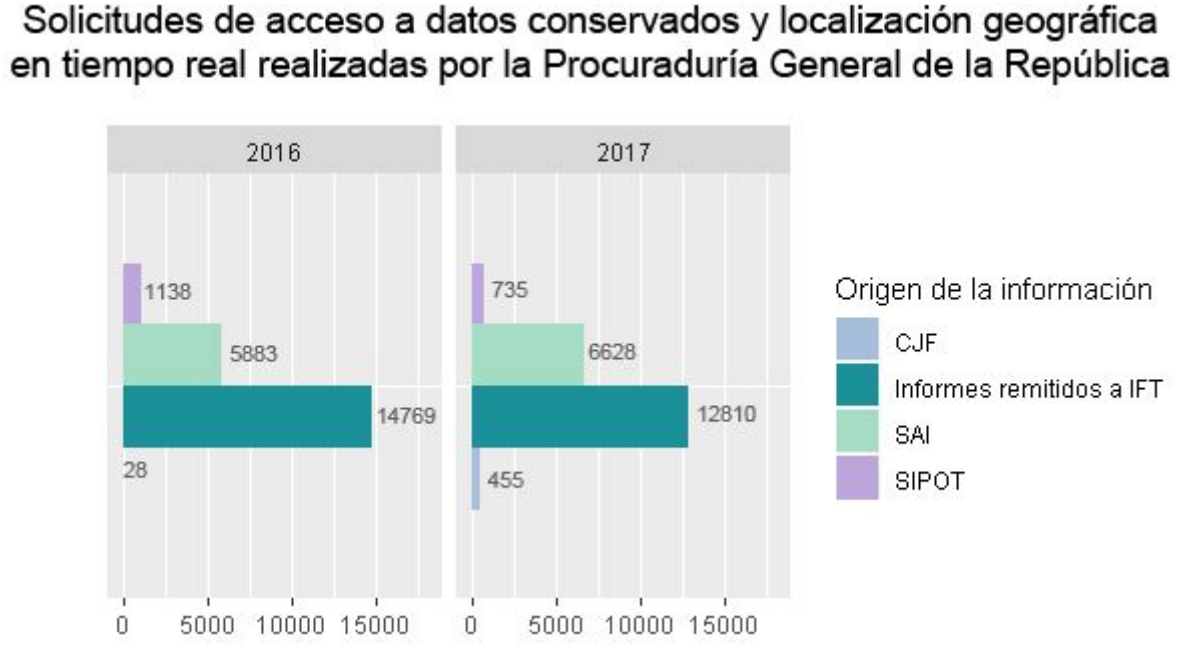
Gráfica 6. Fuente: realización propia con datos de los informes remitidos al IFT por empresas de telecomunicaciones en 2016 y 2017 y solicitudes de acceso a la información.



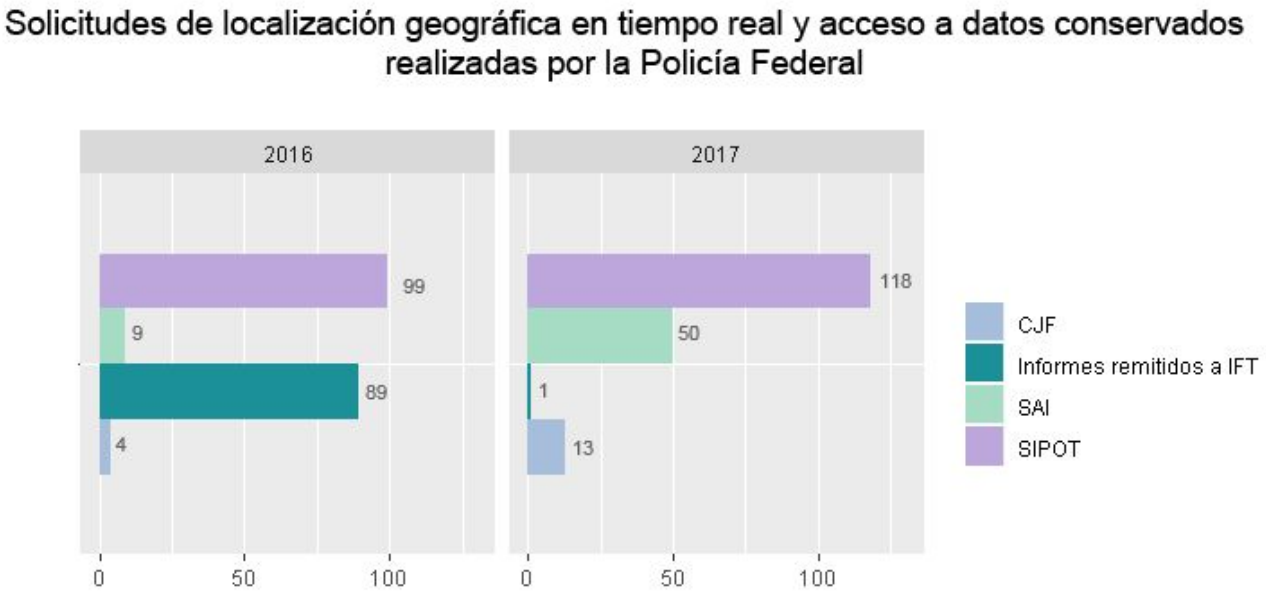
Gráfica 7. Fuente: realización propia con datos de los informes remitidos al IFT por empresas de telecomunicaciones en 2016 y 2017 y solicitudes de acceso a la información.



Gráfica 8: Fuente: realización propia con datos de los informes remitidos al IFT por empresas de telecomunicaciones en 2016 y 2017 y solicitudes de acceso a la información.



Gráfica 9. Fuente: realización propia con datos de los informes remitidos al IFT por empresas de telecomunicaciones en 2016 y 2017, solicitudes de acceso a la información y los publicados en la Plataforma Nacional de Transparencia.



Gráfica 10. Fuente: realización propia con datos de los informes remitidos al IFT por empresas de telecomunicaciones en 2016 y 2017, solicitudes de acceso a la información y los publicados en la Plataforma Nacional de Transparencia.

3. Remoción de obligaciones de transparencia de IFT.

En abril del 2018 el Instituto Federal de Telecomunicaciones eliminó la obligación con la que a partir de 2016 contaban las empresas de telecomunicaciones de remitir informes sobre la colaboración en materia de seguridad y justicia[17]. Dichos informes, remitidos de manera semestral, contenían información sobre el número de solicitudes recibidas por parte de cada autoridad para tener acceso a datos conservados y para ejercer la localización geográfica en tiempo real de los usuarios de telecomunicaciones, así como también el número de dichas solicitudes que fueron entregadas y negadas.

Si bien los informes remitidos en los años 2016 y 2017 contenían información confusa, puesto que no es posible conocer la identidad de las autoridades solicitantes en alrededor el 30% de las solicitudes reportadas, a partir de dichos informes se desprenden datos que muestran prácticas de empresas de telecomunicaciones que deben ser investigadas y en caso de existir abusos al tratamiento de datos personales, sancionadas.

Entre las irregularidades que se desprenden de dichos informes está la entrega de datos de usuarios en el 75 por ciento de los casos en que fueron solicitadas por autoridades no facultadas[18]. Entre dichos casos se entregó información a los gobiernos del Estado de Colima y del Estado de México, los Institutos electorales del Estado de Oaxaca y de la Ciudad de México y a las secretarías de Marina y de Comunicaciones y Transportes.

[17] Lineamiento décimo octavo de los Lineamientos de Colaboración en Materia de Seguridad y Justicia y modifica el plan técnico fundamental de numeración expedidos por el Instituto Federal de Telecomunicaciones, publicados el 2 de diciembre del 2015 en el Diario Oficial de la Federación.
[18] Entre 2016 y 2017 se entregó información de usuarios de telecomunicaciones a empresas no facultadas en 39 ocasiones.

Por otra parte, el hecho de que las empresas de telecomunicaciones hayan entregado la información solicitada en el 94 por ciento de los casos en los años 2016 y 2017, contrastado con que más de la mitad de las solicitudes reportadas por las autoridades mediante solicitudes de acceso a la información fueron realizadas en el mismo periodo de manera excepcional y no fueron ratificadas de manera total por la autoridad judicial, levanta sospechas sobre la existencia de una gran cantidad de abusos. El caso de Telcel y Telmex, quienes entregaron la información de sus usuarios en la totalidad de las solicitudes recibidas es especialmente sospechoso.

La remoción de la obligación de transparencia con la que contaban las empresas de telecomunicaciones es un importante retroceso en materia de transparencia puesto que con ella se pierde acceso a información que permite tener un panorama general sobre la colaboración entre las empresas de telecomunicaciones y las autoridades en materia de vigilancia que de otra manera no se puede conocer.

4. Incumplimiento en la entrega de información pública (caso CISEN-INAI)

Existe una gran resistencia por parte de autoridades tanto locales como federales para ser transparentes y rendir cuentas respecto de sus labores de vigilancia. R3D ha realizado alrededor de 1,300 solicitudes, mediante el ejercicio ejercicio del derecho de acceso de acceso a la información, con el objetivo de obtener datos estadísticos sobre el número de veces que se ha ejercido vigilancia, el número de personas que se ha vigilado, la duración de dichas medidas, entre otros datos. Sin embargo, en la mayoría de los casos las autoridades han negado el acceso a dicha información alegando que su difusión pone en peligro las investigaciones, la seguridad pública e incluso la seguridad nacional.

Tal vez el caso más notorio de opacidad ha sido el del Centro de Investigación y Seguridad Nacional (CISEN) quien ante una solicitud de acceso a la información reservó el número de personas y dispositivos sujetos a una intervención de comunicaciones privadas en el año 2014. Ante dicha negativa R3D impuso un recurso de revisión registrado con el número de folio RDA 2149/16, el cual fue resuelto por el INAI en el sentido de mandar al CISEN la entrega del número de personas vigiladas en 2014.

Sin embargo, la Consejería Jurídica del Ejecutivo Federal interpuso ante la Suprema Corte de Justicia de la Nación un recurso de revisión a la resolución del recurso de revisión, alegando que divulgar el dato sobre el número de personas vigiladas en 2014 por el CISEN ponía en peligro la Seguridad Nacional. En resolución a dicho recurso, registrado con el número de folio 1/2016, la SCJN confirmó la publicidad de la información en el sentido de que divulgar el número de personas y dispositivos intervenidos por el CISEN en 2014 “no estaría haciendo pública información reservada relacionada con las actividades, procesos,

métodos o tecnologías utilizadas por el Centro, ni del producto material de ejecución de una intervención"[19].

Hasta la fecha de la publicación del presente reporte la opacidad sobre el número de personas y dispositivos vigiladas por el CISEN en 2014 persiste puesto que el Centro no ha otorgado dicha información en violación del derecho al acceso a la información y contraviniendo lo mandado tanto por el INAI como por la SCJN.

5. Casos de reserva de información pública relativa al ejercicio de vigilancia

El acceso a las versiones públicas de solicitudes para ejercer vigilancia y las correspondientes resoluciones del poder judicial permite en primer lugar, tener certeza documental respecto del número de solicitudes de ejerciendo la vigilancia realizadas por las autoridades facultadas, número de éstas que fueron autorizadas y no autorizadas, el número de personas o dispositivos vigilados, la duración de las medidas de vigilancia así como los motivos generales de las solicitudes. En segundo lugar, nos permiten conocer cómo se ejerce la vigilancia en los casos en los que por uno u otro motivo las autoridades no otorgan los datos estadísticos relacionados.

Por último, el acceso a dichas versiones públicas permite conocer cuál es la interpretación que el poder judicial dá a las leyes en materia de vigilancia. La falta de claridad de las leyes que contienen medidas de vigilancia produce incertidumbre sobre su aplicación tanto en autoridades, actores del sector privado y en la ciudadanía, contribuyendo a construir un campo fértil para que se den abusos. En éste panorama de incertidumbre legal, la interpretación judicial de dichas leyes equivale en muchos casos a la definición de los alcances, límites y las facultades de vigilancia con las que cuentan las autoridades.

Es por éstos factores que R3D ha solicitado dichas versiones públicas. Desafortunadamente, en la mayoría de los casos autoridades tanto del poder judicial como del ejecutivo han reservado totalmente las versiones públicas, alegando que su divulgación pone en peligro la seguridad de las investigaciones y de las personas involucradas, la viabilidad de las herramientas de vigilancia con las que cuenta el estado, o simplemente, sustentando la reserva en que los documentos solicitados forman parte de una investigación en curso.

La publicidad de dicha información ha sido reconocida por algunos organismos garantes del derecho de acceso a la información al poner en riesgo la viabilidad de las investigaciones, ni la seguridad en ningún momento puesto que ésta información no revela datos que identifiquen a las personas y/o a los dispositivos vigilados, ni datos específicos que permitan conocer las circunstancias bajo las que se conducen las investigaciones. Sin embargo también existen interpretaciones de organismos garantes contrarias al derecho a la

[19] Pleno, SCJN, Resolución al Recurso de Revisión en Materia de Seguridad Nacional 1/2016 de fecha 05 de diciembre de 2016, disponible en: http://www2.scjn.gob.mx/ConsultaTematica/PaginasPub/DetallePub.aspx?AsuntoID=202248

información, como la del INAI quien argumentó la reserva total de la información solicitada al CISEN e inclusive determinó que de acuerdo al artículo 51 de la Ley de Seguridad Nacional, dicha reserva no necesitaba de una prueba de daño.

E. Reducida efectividad de la vigilancia en investigación de delitos

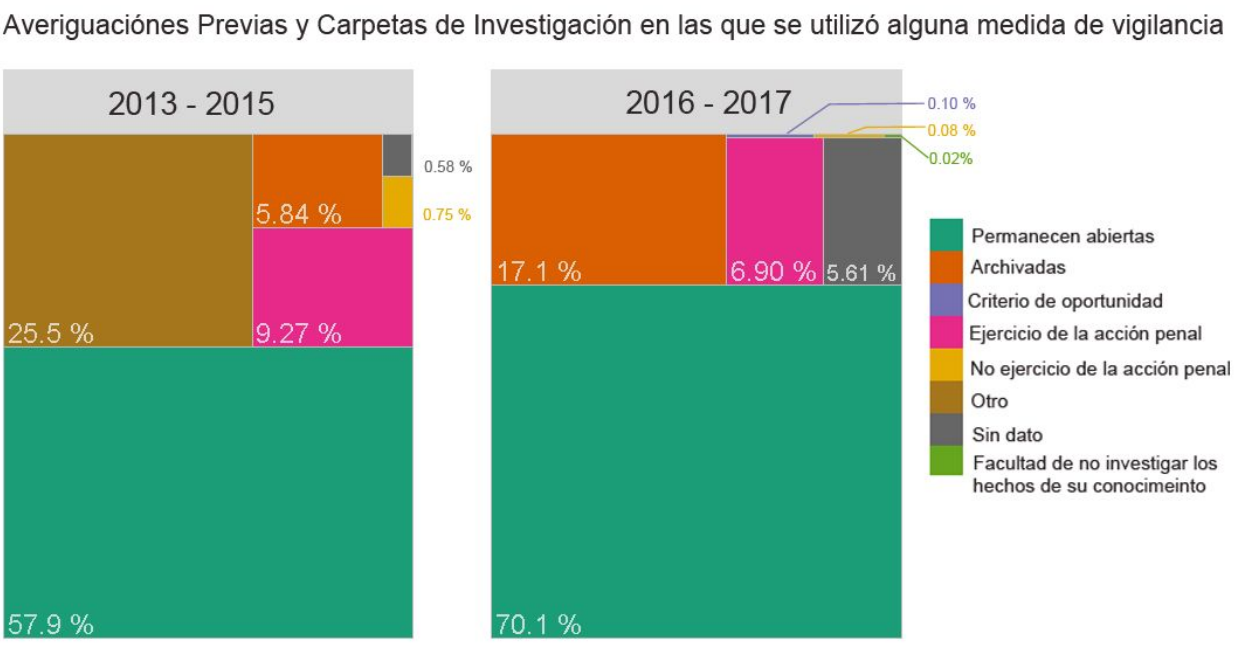
Otra de las perspectivas desde las cuáles es necesario analizar la vigilancia, al ser ésta parte de las políticas públicas, es desde la efectividad de la misma en la investigación de delitos. En México, como ocurre en el resto del mundo, el uso de vigilancia se ha tratado de justificar como una medida necesaria y de gran efectividad en la provisión de seguridad -inclusive cuando su utilización presupone la violación del derecho a la privacidad así como la erogación de enormes cantidades del gasto público- sin que se analice dicha necesidad y efectividad.

1. Esfuerzo por medir su efectividad: datos sobre el resultado de averiguaciones previas en las que se utilizó la vigilancia.

Actualmente no existen indicadores de desempeño como ocurre con otras formas de ejercicio del presupuesto, que permitan medir el éxito que tienen las labores de vigilancia. Desde el punto de vista de evaluación de políticas públicas, la vigilancia también se encuentra fuera de toda supervisión. Esta excepcionalidad es otro de los factores que permite que la vigilancia se emplee de manera arbitraria y que se adquiera de manera injustificada herramientas de vigilancia en un contexto de irregularidades y corrupción.

En un esfuerzo por abordar el tema de la vigilancia estatal desde la perspectiva de su efectividad, R3D solicitó datos estadísticos a la Procuraduría General de la República, y a las procuradurías y fiscalías locales, sobre el número de averiguaciones previas y carpetas de investigación en las que se practicó vigilancia junto con datos sobre el resultado de las mismas, entre los años 2013 a 2017.

Lo que demuestran los datos entregados por las autoridades facultadas en vigilancia es que a la fecha en que se realizaron las solicitudes (los años 2016 y 2018) de acceso a la información para los dos periodos de estudio (del año 2013 al 2015 y del año 2016 al 2017 respectivamente) sólamente en el 8.28% por ciento de las averiguaciones previas(AP) y carpetas de investigación(CI) en que se utilizó alguna medida de vigilancia resultaron en el ejerció la acción penal. Por otra parte el 63 por ciento de las AP y las CI en las que se utilizó alguna medida de vigilancia permanecían abiertas.



Gráfica 11. Fuente: realización propia con datos obtenidos mediante solicitudes de acceso a la información.

Entre los casos en los que el uso de vigilancia por parte de autoridades no ha sido efectivo en la resolución de delitos, sobresalen los casos de las fiscalías generales de los estados de Puebla y de Yucatán las cuales respondieron en 2016 y 2018, haber ejercido acción penal en sólo el 3 y el 5 por ciento, respectivamente, de las AP y CI en las que utilizó alguna medida de vigilancia entre los años 2013 y el 2017.

Gráfica 12. Fuente: realización propia con datos obtenidos mediante solicitudes de acceso a la información.

Gráfica 13. Fuente: realización propia con datos obtenidos mediante solicitudes de acceso a la información.

F. Casos documentados de abuso de la vigilancia

1. Espionaje a defensorxs de derechos humanos, periodistas y otras víctimas.

Se han documentado varias instancias en las que la vigilancia, y en particular, herramientas de malware de vigilancia han sido utilizadas en contra de disidentes, periodistas y defensores de derechos humanos.

En febrero de este año, se dió a conocer que el Estado Mexicano utilizó *malware* de vigilancia desarrollado por la empresa israelí NSO Group, 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 El Poder del Consumidor. Los ataques perpetrados contra los activistas tuvo lugar mientras se planeaba una campaña en favor del impuesto a las bebidas azucaradas[20].

[20] Perlroth, Nicole (11 de febrero de 2017) Spyware's Odd Targets: Backers of Mexico's Soda Tax. The New York Times. Disponible en: https://www.nytimes.com/2017/02/11/technology/hack-mexico-soda-tax-advocates.html?smid=fb-share&_r=0 ; Scott-Railton, John. Marczak, Bill. Guarnieri, Claudio. Crete-Nishihata, Masashi. 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/

En Junio de 2017, Citizen Lab, así como ARTICLE 19, la Red en Defensa de los Derechos Digitales (R3D) y SocialTIC publicaron el informe **"Gobierno Espía: Vigilancia sistemática a periodistas y defensores de derechos humanos en México"**[21], en la cual se da cuenta de múltiples casos de intentos de infección con el malware *Pegasus*.[22]

En total se han documentado más de 100 mensajes de texto con enlaces que dirigen a dominios identificados como parte de la estructura de NSO. Esto implica que los mensajes analizados corresponden sin lugar a dudas a intentos de infección con el malware Pegasus.

Entre las más de 20 personas y organizaciones que ha sido documentado que recibieron mensajes con la intención de infectar sus dispositivos con el malware *Pegasus* incluye a defensores de derechos humanos, periodistas, activistas anticorrupción e incluso menores de edad:

- **Centro Miguel Agustín Pro Juárez (Centro Prodh):** Entre los meses de abril y junio del año 2016, tres personas dentro de la organización recibieron mensajes que se ha confirmado constituyen intentos de infección con el malware de espionaje Pegasus. Los mensajes fueron recibidos en fechas clave dentro del trabajo de defensa de derechos humanos que el Centro Prodh ha realizado en casos de alto impacto como la desaparición forzada de 43 estudiantes de Ayotzinapa, la masacre de Tlatlaya y los casos de tortura sexual en Atenco.

[21] Disponible en: https://r3d.mx/gobiernoespia/
[22] Ver también: Ahmed, Azam. Perlroth, Nicole. (June 19, 2017) Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families. The New York Times. Disponible ent: https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html

- **Aristegui Noticias (Carmen Aristegui, Emilio Aristegui, Rafael Cabrera y Sebastián Barragán):** Se documentaron mensajes recibidos en los años 2015 y 2016 por Carmen Aristegui, por su hijo Emilio y por integrantes de su equipo de investigación como Sebastián Barragán y Rafael Cabrera. En los últimos años, la actividad periodística de Aristegui Noticias ha revelado casos de corrupción como el reportaje de la Casa Blanca[23] o exponer una red de prostitución[24] que operaba desde las oficinas del PRI en la Ciudad de México. Además, ha hecho reportajes sobre casos de violaciones graves a derechos humanos en México como la desaparición forzada de los 43 estudiantes normalistas de Ayotzinapa[25].

  Es importante enfatizar que al momento de recibir los mensajes, Emilio era menor de edad. Lo anterior representa el primer ataque documentado con este malware contra un familiar directo de un objetivo y, en total, se fueron contabilizados más de 40 intentos contra el hijo de la periodista.

- **Carlos Loret de Mola (Periodista):** Periodista de radio, televisión y columnista impreso. Su programa de televisión "Despierta con Loret" (antes "Primero Noticias") es el noticiario con mayor audiencia en el país. Se ha documentado que entre agosto de 2015 a abril de 2016 recibió al menos 8 mensajes que pretendían infectar su dispositivo con el malware Pegasus. El primero de los mensajes fue recibido el mismo día que el periodista publicó[26] un reportaje sobre ejecuciones extrajudiciales en Tanhuato, Michoacán.

- **Instituto Mexicano por la Competitividad (IMCO):** Se ha documentado que el Director de la organización, Juan Pardinas y otra integrante de dicha organización, Alexandra Zapata, recibieron mensajes intentando infectar su dispositivo. IMCO ha sido una de las organizaciones que ha liderado esfuerzos de incidencia para la reforma legal anticorrupción, en particular ha impulsado la ley conocida como "Ley 3

---

[23] Cabrera, R., D. Lizárraga, I. Huerta y S. Barragán (9 de noviembre de 2014) "La casa blanca de Enrique Peña Nieto (investigación especial)". Aristegui Noticias. Disponible en: http://aristeguinoticias.com/0911/mexico/la-casa-blanca-de-enrique-pena-nieto/

[24] "Video: Opera #RedProstitución en PRI-DF (investigación)" (2 de abril de 2014) Aristegui Noticias. Disponible en: http://aristeguinoticias.com/0204/mexico/opera-redprostitucion-en-pri-df-investigacion-mvs/

[25] "Caso Iguala: 1 mes y no aparecen los 43 estudiantes" (24 de octubre de 2014) Aristegui Noticias. Disponible en: http://aristeguinoticias.com/2410/mexico/caso-iguala-1-mes-y-no-aparecen-los-43-estudiantes/

[26] Loret de Mola, C. (5 de agosto de 2015) "Nueva ejecución extrajudicial". El Universal. Disponible en:http://www.eluniversal.com.mx/entrada-de-opinion/columna/carlos-loret-de-mola/nacion/2015/08/5/nueva-ejecucion-extrajudicial; (1 de septiembre de 2015) "Tanhuato: las pruebas que hacen tropezar al gobierno (I)". El Universal. Disponible en:http://www.eluniversal.com.mx/entrada-de-opinion/columna/carlos-loret-de-mola/nacion/2015/09/1/tanhuato-las-pruebas-que-hacen

de 3”[27], la cual generó gran resistencia y ataques por parte de fuerzas políticas asociadas al gobierno federal.

- **Mexicanos Contra la Corrupción y la Impunidad (MCCI):** Se ha documentado que los periodistas Salvador Camarena y Daniel Lizárraga, Director General de Investigación Periodística y Jefe de Información de la organización respectivamente, recibió al menos 3 mensajes con malware de NSO en el año 2016. Salvador Camarena y Daniel Lizárraga en el pasado también fueron parte de Aristegui Noticias y participaron en investigaciones como la de revelación de los Panama Papers. Igualmente, el 30 de agosto de 2017 se revelaron ataques con el malware *Pegasus* en contra del Director de la organización, Claudio X. González[28] y fueron reveladas otras formas de intimidación por parte del gobierno federal en el periódico *The New York Times*[29].

Aunado a lo anterior, el pasado 10 de julio Citizen Lab de la Universidad de Toronto ha confirmado en un nuevo informe[30], publicado también por el New York Times[31], que un teléfono del **Grupo Interdisciplinario de Expertos Internacionales (GIEI)** recibió mensajes de texto vinculados a la infraestructura del malware Pegasus; el envío de los mensajes de texto con enlaces maliciosos ocurre alrededor de uno de los casos más sensibles para el gobierno federal: la investigación sobre la desaparición forzada de 43 estudiantes (caso Ayotzinapa) lo que confirma la constante obstaculización por parte del gobierno federal en contra del grupo de expertos que puso en tela de juicio la llamada “verdad histórica” de la PGR en el caso Ayotzinapa, además de haber sido objeto de una constante campaña de descalificación para inhibir su labor.

Es importante resaltar que durante las fechas en que los periodistas, científicos, activistas y defensores de derechos humanos recibieron los mensajes, estos se encontraban en coyunturas críticas de trabajo periodístico y de defensa de derechos humanos que les confrontaba con un actor común: el Gobierno Federal.

---

[27] Cortés, J., Kaiser, M., Roldán, J. et al. (febrero de 2016) Iniciativa ciudadana de Ley general de responsabilidades administrativas.
Disponible en: http://ley3de3.mx/wp-content/uploads/2016/02/Ley3de3_LEY_IniciativaCiudadanaDeLeyGeneralDeResponsabilidadesAdministrativas_Documento.pdf

[28] Scott-Railton, John. Marczak, Bill. Razzak, Bahr Abdul. Crete-Nishihata, Masashi. Deibert, Ron. RECKLESS V: Director of Mexican Anti-Corruption Group Targeted with NSO Group’s Spyware. The Citizen Lab. Disponible en: https://citizenlab.ca/2017/08/nso-spyware-mexico-corruption/

[29] Ahmed, Azam. (August 30, 2017) Un empresario activista lucha contra la corrupción en México y se convierte en un blanco del Estado. The New York Times. Disponible en: https://www.nytimes.com/es/2017/08/30/mexico-pegasus-claudio-x-gonzalez-laporte-enrique-pena-nieto-corrupcion/

[30] Scott-Railton, John. Marczak, Bill. Razzak, Bahr Abdul. Crete-Nishihata, Masashi. Deibert, Ron. RECKLESS III: Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware. The Citizen Lab. Disponible en: https://citizenlab.ca/2017/07/mexico-disappearances-nso/

[31] Ahmed, Azam. (July 10, 2017) Spyware in Mexico Targeted Investigators Seeking Students. The New York Times. Available at: https://www.nytimes.com/2017/07/10/world/americas/mexico-missing-students-pegasus-spyware.html

2. Impunidad en casos de abuso.

La denuncia de #GobiernoEspía fue presentada el 19 de junio de 2017 ante la PGR, específicamente ante la Fiscalía Especializada en Atención de Delitos cometidos contra la libertad de expresión (FEADLE). La carpeta de investigación correspondiente fue asignada al expediente FED/SDHPDSC/U-NAI-CDMX/0000430/2017. Notoriamente, poco más de un año después de haberse denunciado, la investigación ha presentado prácticamente nulos avances. Incluso, las y los denunciantes tuvieron que acudir ante un juez de distrito para impugnar diversas decisiones de la FEADLE encaminadas a desestimar varias de las pruebas ofrecidas por las víctimas. Al resolver una de estas impugnaciones, la número 19/2008 específicamente, el juez de distrito correspondiente determinó que la línea de investigación debía centrarse en la adquisición y posterior uso ilegal de Pegasus por parte de la a Agencia de Investigación Criminal, adscrita a la PGR, al haber quedado acreditado nuevamente en el desarrollo de la audiencia en cuestión que dicho malware fue adquirido al menos por esta instancia. Asimismo, el juez remarcó el derecho de las víctimas a participar en la investigación y la obligación de la PGR de conducirse con debida diligencia, señalando que no debía trasladar la carga de la prueba a las víctimas. No conforme, la PGR solicitó la reserva de información que derivase de la investigación ordenada con motivo de de dicha audiencia, bajo el argumento de una supuesta afectación a la seguridad nacional; solicitud que fue negada por el juez.

3. Falta de mecanismo independiente de investigación de los casos de abuso.

Desde una perspectiva más general, de acuerdo a los estándares internacionales en materia de derechos humanos y a los principios generales de derecho, ante cualquier violación de derechos humanos, el poder acceder a un juicio justo, por un tribunal independiente e imparcial, establecido por la ley, es un derecho absoluto y sin excepciones en su aplicación.[32] En este sentido, el artículo 10 de la Declaración Universal de los Derechos Humanos señala que toda persona tiene derecho, en **condiciones de plena igualdad,** a ser oída públicamente y con justicia por un **tribunal independiente e imparcial**, para la determinación de sus derechos y obligaciones o para el examen de cualquier acusación contra ella en materia penal.

De igual forma, reafirmando la importancia y el carácter fundamental de este derecho, la necesidad de que en todo proceso se establezcan las debidas garantías de competencia, independencia e imparcialidad, se encuentra prevista en los artículos 14(1) del Pacto Internacional de Derechos Civiles y Políticos, 8 de la Convención Americana sobre Derechos Humanos, 6(1) del Convenio Europeo de

[32] https://www.amnesty.org/download/Documents/8000/pol300022014es.pdf

Derechos Humanos, 20(1) del Estatuto del Tribunal Penal Internacional para la ex Yugoslavia, 19(1) del Estatuto del Tribunal Penal Internacional para Ruanda así como (64)2 y 72(1) del Estatuto de Roma para la Corte Penal Internacional.

Entonces, para una investigación efectiva del uso abusivo de este tipo de herramientas, la independencia e imparcialidad del tribunal que conozca del caso son esenciales y constituyen un requisito previo del principio de legalidad[33] además de ser fundamentales para que se mantenga el respeto por la administración de la justicia[34]. El deber de imparcialidad por su parte implica que cada una de las personas que participan en la toma de decisiones en un proceso penal **sean imparciales y parezcan serlo[35].** Esto es, que los jueces y los jurados **no tengan ningún interés en la causa** y no actúen de tal forma que favorezcan los intereses de alguna de las partes[36]. Tomando como referencia el caso de #GobiernoEspía y lo que fue desarrollado en este sentido durante el apartado anterior, es claro que a la fecha en México el escenario ha sido todo lo contrario.

Lo anterior es sumamente relevante considerando que de acuerdo a los estándares internacionales, si una persona involucrada en un proceso penal no puede tomar imparcialmente una decisión al respecto o si así lo parece, "lo normal es que se declare incompetente"[37]. Incluso, la Corte Interamericana de Derechos Humanos ha establecido que el derecho a recusar a un tribunal, a un juez o a miembros de un jurado por falta de independencia o imparcialidad es necesario para garantizar el respeto del derecho a un tribunal independiente e imparcial y **los Estados deben garantizar que se dispone de un mecanismo con tal fin**[38]. No obstante, en México no existe un mecanismo de esa naturaleza. Tampoco existe uno que garantice la independencia e imparcialidad necesarias para llevar a cabo una investigación efectiva en torno a la utilización de herramientas de vigilancia estatal en el país.

Como prueba de ello, además de lo anteriormente mencionado, los Relatores Especiales recordaron en su informe que desde julio de 2017, expertos de la ONU instaron a México a llevar a cabo una investigación independiente e imparcial respecto de la adquisición y uso del programa Pegasus. Asimismo, remarcaron que toda investigación debe ser independiente del gobierno para demostrar que efectivamente se comprenden y se respetan los principios de debido proceso y Estado de derecho que deben regir en toda sociedad democrática.

---

[33] Principio 1 de los Principios de Bangalore.

[34] Observación general 32, Comité de Derechos Humanos, párr. 21; Tribunal Europeo: Piersack vs. Belgium (8692/79) (1982), párrs. 30-32, Sander vs. United Kingdom (34129/96) (2000), párr. 22,Galstyan vs. Armenia (26986/03) (2007), párr. 79; Apitz Barbera y otros vs. Venezuela, Corte Interamericana (2008), párr. 56;Prosecutor vs. Anto Furundžija (IT-95-17/1-A), Sala de Apelaciones del TPIY (julio de 2000), párrs. 189 y 190; ver también https://www.amnesty.org/download/Documents/8000/pol300022014es.pdf

[35] Comité de Derechos Humanos: Karttunen vs. Finlandia, Doc. ONU: CCPR/C/OP/4: CCPR/C/46/D/387/1989 (1992), párr. 7.2-3, Collins vs. Jamaica, Doc. ONU: CCPR/C/OP/4: CCPR/C/43/ D/240/1987 (1991), párr. 8.

[36] Principio 2 de los Principios de Bangalore; Karttunen vs. Finlandia, Comité de Derechos Humanos, Doc. ONU: CCPR/C/OP/4: CCPR/C/46/D/387/1989 (1992), párr. 7.2.

[37] Principios 2.5 y 4.4 de los Principios de Bangalore; Recomendación CM/Rec (2010) 12, Consejo de Europa, párrs. 59-60; Palamara Iribarne vs. Chile, Corte Interamericana (2005), párrs. 145-147 y 158-161.

[38] Apitz Barbera y otros vs. Venezuela, Corte Interamericana (2008), párrs. 63-67.

Por tanto, de conformidad con lo externado por los Relatores, el Estado mexicano debe no solo analizar e investigar exhaustivamente a todos los potenciales compradores y usuarios de Pegasus así como todas las fuentes de información que puedan demostrar la operación de este programa espía sino también brindar al público información actualizada y periódica respecto del estado de la investigación, garantizando que la misma goce de las debidas salvaguardas de imparcialidad e independencia. Además, la PGR debe acatar la resolución del INAI de fecha 31 de enero de 2018 misma que le instruye a dar a conocer los contratos relacionados con la adquisición de Pegasus y que también ha sido "enérgicamente" suscrita por los Relatores.

Por último, como también fue señalado por ellos, resulta evidente la necesidad de que en México se establezca un marco legal adecuado, acorde a los estándares internacionales en la materia, para evitar injerencias arbitrarias o clandestinas en contra de la privacidad de las personas, el cual deberá incluir garantías y medidas de supervisión judicial independiente como ya se mencionó.

Incluso, respecto de este último punto, como también ha sido específicamente recomendado por los Relatores, México debe considerar la creación de un órgano independiente encargado de supervisar efectivamente la forma en que el Estado ejerce funciones de vigilancia.

4. Respuesta del Estado mexicano a recomendaciones sobre #GobiernoEspía

Notoriamente, ante las Recomendaciones de los Relatores y lo señalado con anterioridad, la postura del Estado mexicano sigue siendo la de subestimar la gravedad de los hechos de espionaje, desconociendo también la necesidad de que se implementen las garantías de imparcialidad e independencia necesarias para la investigación efectiva del caso.

Para empezar, en su respuesta oficial el gobierno mexicano señaló que "ha atendido la mayor parte de las diligencias propuestas" por los denunciantes. No obstante, la realidad es que de aproximadamente 70 pruebas ofrecidas por la defensa, la PGR ha desahogado cerca de nueve, negando expresamente las 49 restantes. Además, el Estado mexicano "enfatizó" que los denunciantes han tenido y tendrán acceso permanente a la carpeta de investigación; sin embargo, la PGR no solo ha negado copia del expediente a los denunciantes sino también, argumentando supuestas afectaciones a la seguridad nacional (¿?) ha solicitado la reserva de diversa información; por ejemplo, aquella que derive de su investigación en torno a la uso y adquisición de Pegasus por parte de la AIC.

No conforme, pretendiendo justificar la independencia e imparcialidad de la investigación sobre el caso, el gobierno señaló que ha organizado un grupo de apoyo técnico conformado por representantes de: i) la Unión Internacional de Telecomunicaciones (UIT), organismo especializado en telecomunicaciones de la Organización de Naciones Unidas; ii) la

Asociación Mundial de Operadores Móviles (GSMA), con sede en Londres, Reino Unido; iii) la Escuela Superior de Ingeniería Mecánica y Eléctrica del Instituto Politécnico Nacional; iv) El expresidente de la Comisión Federal de Telecomunicaciones, Héctor Osuna Jaime; v) el Buró Federal de Investigaciones (FBI) de los Estados Unidos; vi) Ministerio de Justicia canadiense, vía asistencia jurídica internacional y vii) "Citizen Lab" de la Universidad de Toronto.

Tal señalamiento es insostenible, por decir lo menos. A la fecha, dentro del expediente penal no obra documento alguno que acredite que representantes de las instituciones enlistadas del i) al vi) hayan colaborado de manera alguna con la investigación. Incluso, oficiales estadounidenses de alto rango declararon públicamente que el FBI NO desea colaborar con el gobierno mexicano porque "les preocupa que los mexicanos enaltecieran su participación con la intención de darle una apariencia de credibilidad a lo que consideran una fachada" en tanto dudan que el Estado "realmente quiera resolver el caso, ya que indagarlo a fondo podría comprometer a algunos de sus funcionarios más importantes"[39].

Además, respecto de la número vii), Citizen Lab, es preciso señalar que la PGR se limitó a mandarle a sus representantes un cuestionario sin reconocerle a dicho laboratorio el carácter de perito independiente dentro de la investigación. Inclusive el cuestionario en comento, por la manera en que ha sido traducido al español y los extractos que se han tomado del mismo, a toda luz lo que pretende es desestimar el análisis llevado a cabo por Citizen Lab para concluir que los denunciantes fueron objetos de ataque con Pegasus.

Por último, de manera por demás preocupante, no obstante todo lo que ha sido desarrollado con anterioridad, el Estado "sugirió" a los Relatores "considerar en sus recomendaciones elementos que se orienten a fortalecer el papel de la FEADLE y abonen así a la confianza correspondiente, considerando además que legalmente es la autoridad competente para ello, además que su trabajo se realiza de forma profesional, autónoma y absolutamente imparcial."

[39] https://www.nytimes.com/es/2018/02/20/mexico-fbi-investigacion-pegasus-espionaje/

Nota metodológica

La información sobre el número de solicitudes para ejercer vigilancia reportada por empresas de telecomunicaciones, por las autoridades con facultades de vigilancia y por el consejo de la judicatura proviene de solicitudes de acceso a la información realizadas a las autoridades con facultades de vigilancia así como de los informes remitidos al IFT por empresas de telecomunicaciones. Dicha información puede ser descargada aquí.

Las solicitudes de acceso a la información dirigidas a las autoridades facultadas fueron realizadas en dos periodos: en 2016 para la información concerniente a los años 2013 a 2015 y en 2018 para la información de los años 2016 y 2017. Debido a la resistencia de ciertas autoridades a contestar lo solicitado, a la incompletitud o incoherencia de algunas de sus preguntas no contamos con información completa. Por lo mismo, los datos presentados en el informe no incluye a todas las autoridades. La tabla al final de la presente sección muestra que autoridades fueron consideradas en cada sección del informe en las que se utilizaron datos obtenidos mediante solicitudes de acceso a la información dirigidas a autoridades con facultades de vigilancia.

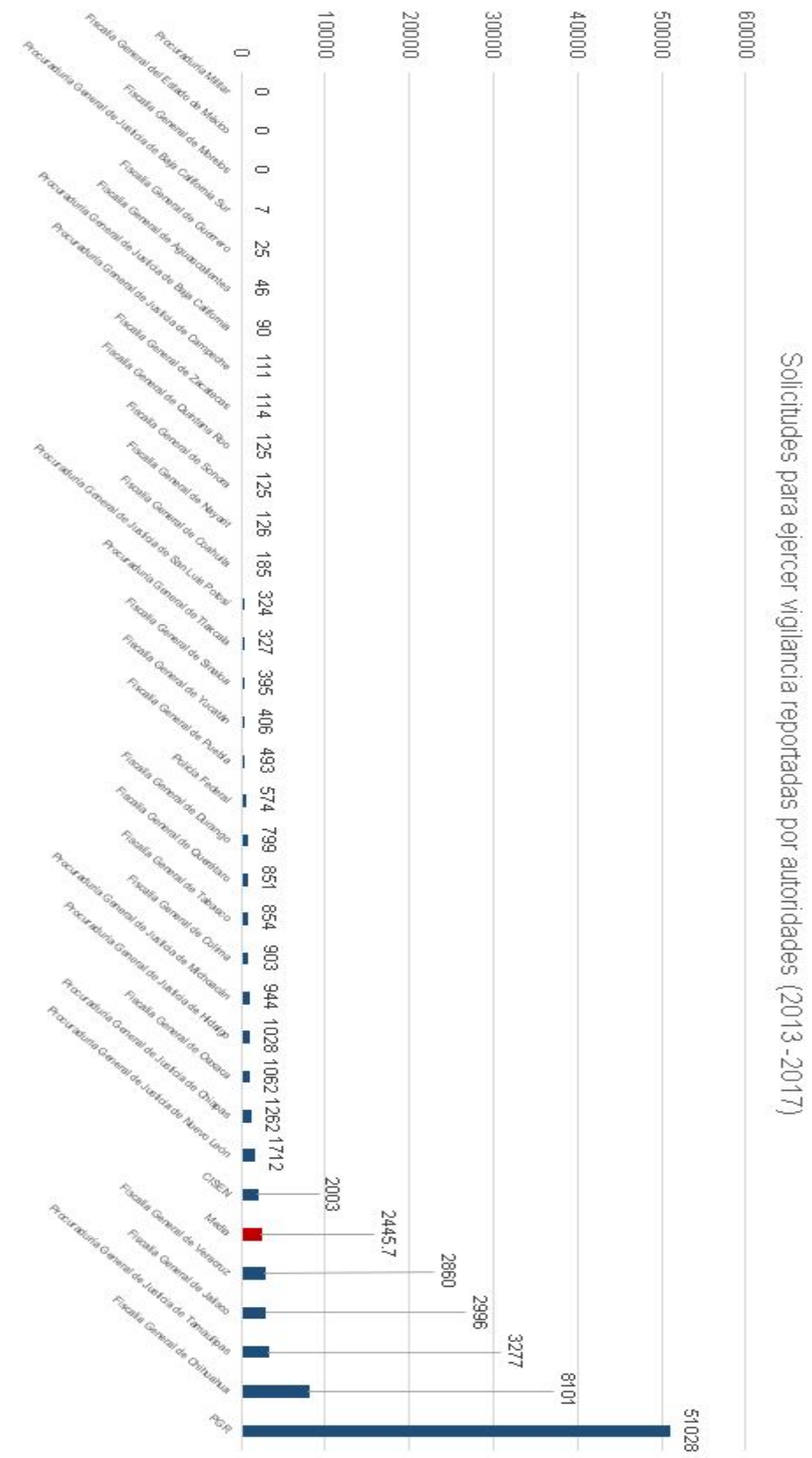
El total de solicitudes enviadas a la autoridad judicial o las realizadas mediante el mecanismo de emergencia se construye, correspondientemente, a partir de la suma de las solicitudes enviadas a la autoridad judicial autorizadas y no autorizadas, y la suma de solicitudes ratificadas totalmente, parcialmente o no ratificadas, excepto en los casos en que los resultados de dichas sumas sean menor a los totales de solicitudes enviadas a la autoridad judicial o las realizadas mediante el mecanismo de emergencia reportadas por las autoridades en sus respuestas. En el segundo caso, la categoría “sin dato” en la gráfica 5 corresponde a la diferencia entre el total de solicitudes reportado por las autoridades y el que surge de la suma de las solicitudes autorizadas, negadas o ratificadas parcialmente, totalmente y no ratificadas.

Las averiguaciones previas (AP) y carpetas de investigación (CI) en las que se reportó ejercicio de acción penal y que permanecen abiertas (al ser imprescriptibles en el caso del delito de secuestro) se contaron como AP o CI en las que se ejerció acción penal.

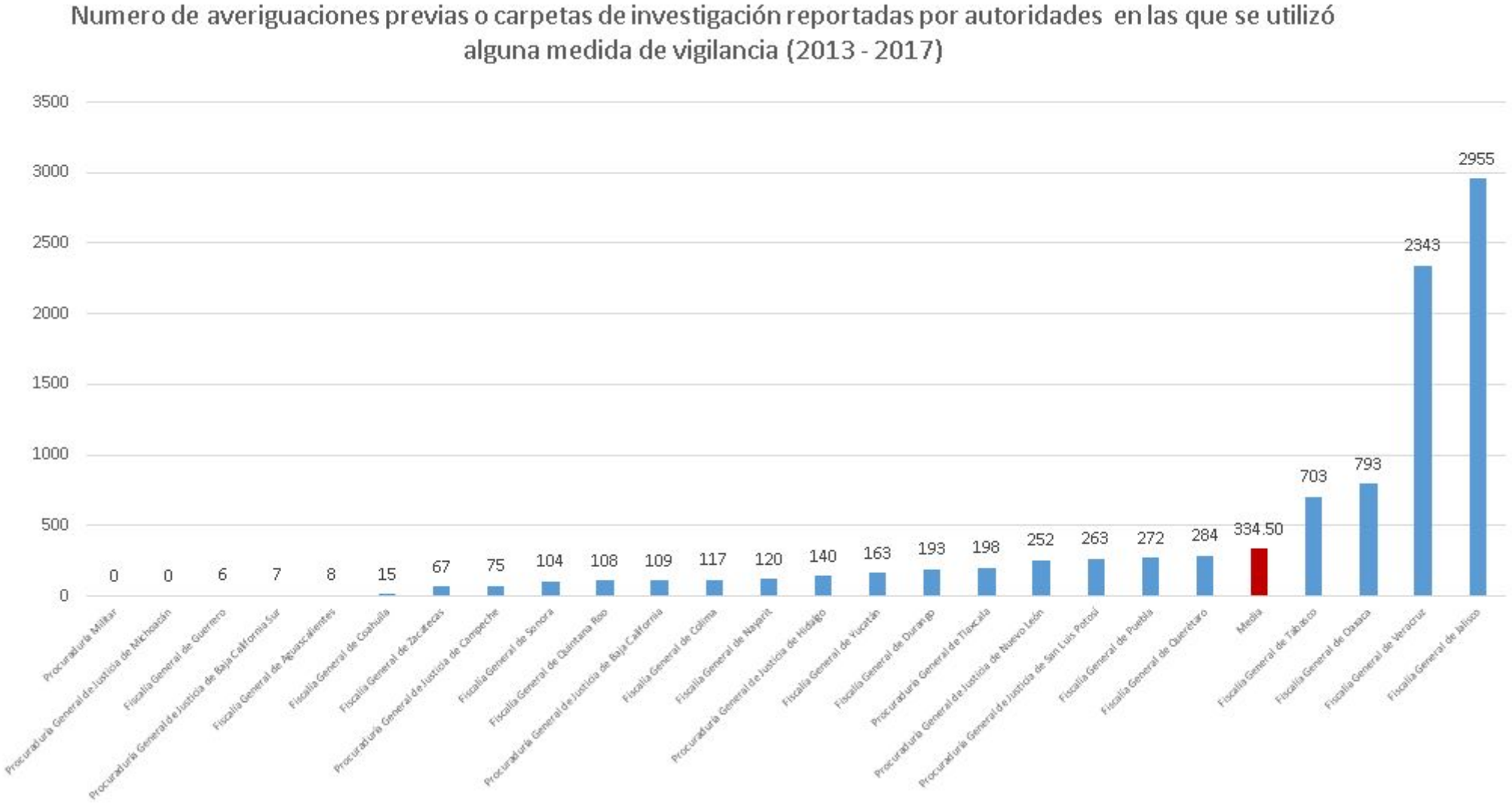
AUTORIDAD	Sección C.1	Sección C.2	Sección D.2, gráficas 6 y 7	Sección E.1 (2013 - 2015)	Sección E.1 (2016 - 2017)
CISEN					
PGR					
Policía Federal					
Procuraduría Militar					
Fiscalía General de Aguascalientes					
Procuraduría General de Justicia de Baja California					
Procuraduría General de Justicia de Baja California					

Sur					
Procuraduría General de Justicia de Campeche					
Procuraduría General de Justicia de Chiapas					
Fiscalía General de Chihuahua					
Procuraduría General de Justicia de la Ciudad de México					
Fiscalía General de Coahuila					
Fiscalía General de Colima					
Fiscalía General de Durango					
Fiscalía General del Estado de México					
Procuraduría General de Justicia de Guanajuato					
Fiscalía General de Guerrero					
Procuraduría General de Justicia de Hidalgo					
Fiscalía General de Jalisco					
Procuraduría General de Justicia de Michoacán					
Fiscalía General de Morelos					
Fiscalía General de Nayarit					
Procuraduría General de Justicia de Nuevo León					
Fiscalía General de Oaxaca					
Fiscalía General de Puebla					
Fiscalía General de Querétaro					
Fiscalía General de Quintana Roo					
Procuraduría General de Justicia de San Luis Potosí					
Fiscalía General de Sinaloa					
Fiscalía General de Sonora					
Fiscalía General de Tabasco					
Procuraduría General de Justicia de Tamaulipas					
Procuraduría General de Tlaxcala					
Fiscalía General de Veracruz					
Fiscalía General de Yucatán					
Fiscalía General de Zacatecas					

Anexo



Gráfica 13: Fuente: solicitudes de acceso a la información


Numero de averiguaciones previas o carpetas de investigación reportadas por autoridades en las que se utilizó alguna medida de vigilancia (2013 - 2017)
3500
3000
2500
2000
1500
1000
500
0
0
0
6
7
8
15
67
75
104
108
109
117
120
140
163
193
198
252
263
272
284
334.50
703
793
2343
2955
Procuraduría Militar
Procuraduría General de Justicia de Michoacán
Fiscalía General de Guerrero
Procuraduría General de Justicia de Baja California Sur
Fiscalía General de Aguascalientes
Fiscalía General de Coahuila
Fiscalía General de Zacatecas
Procuraduría General de Justicia de Campeche
Fiscalía General de Sonora
Fiscalía General de Quintana Roo
Procuraduría General de Justicia de Baja California
Fiscalía General de Colima
Fiscalía General de Nayarit
Procuraduría General de Justicia de Hidalgo
Fiscalía General de Yucatán
Fiscalía General de Durango
Procuraduría General de Tlaxcala
Procuraduría General de Justicia de Nuevo León
Procuraduría General de Justicia de San Luis Potosí
Fiscalía General de Puebla
Fiscalía General de Querétaro
Media
Fiscalía General de Tabasco
Fiscalía General de Oaxaca
Fiscalía General de Veracruz
Fiscalía General de Jalisco