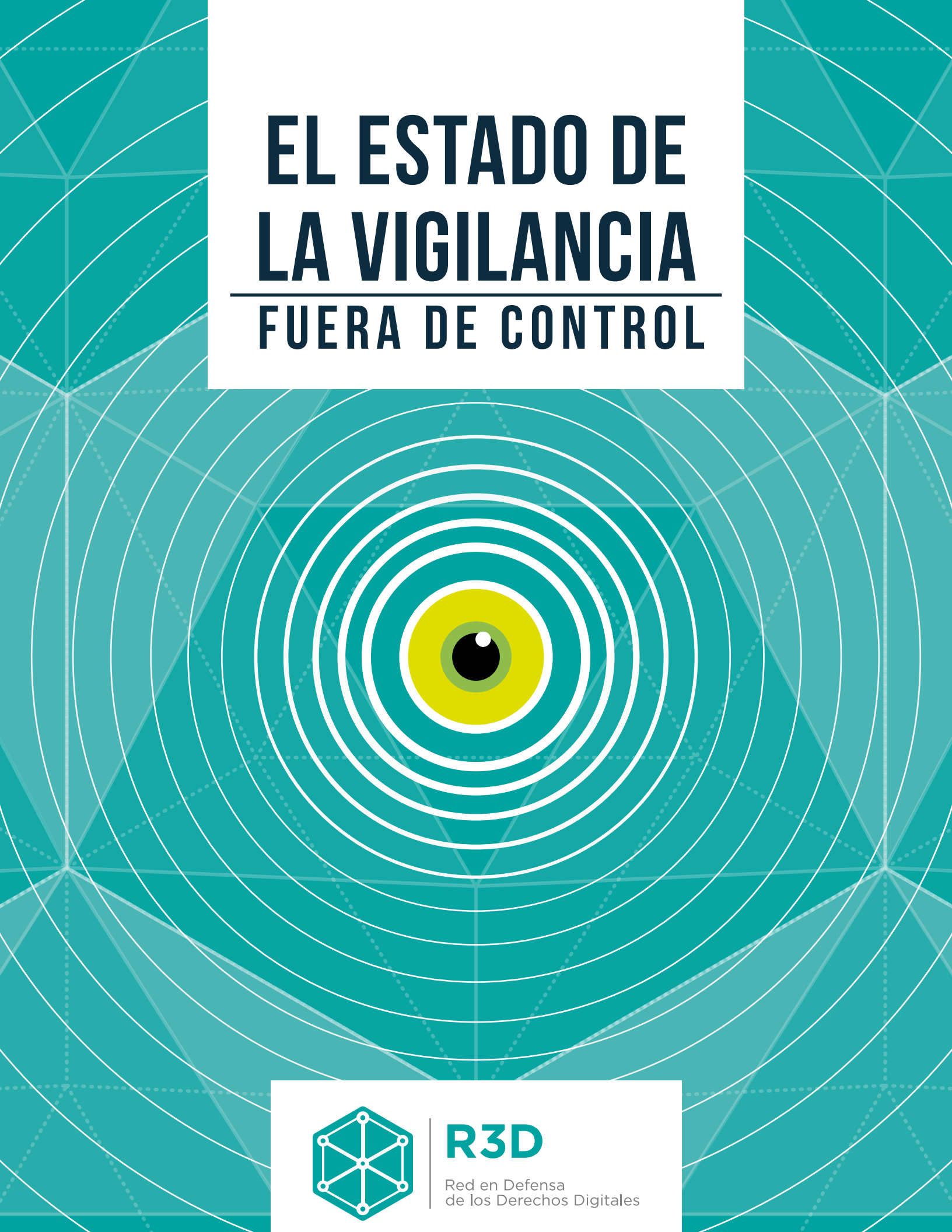
EL ESTADO DE LA VIGILANCIA

FUERA DE CONTROL



R3D
Red en Defensa
de los Derechos Digitales

RED EN DEFENSA DE LOS DERECHOS DIGITALES (R3D):

Organización mexicana sin fines de lucro, dedicada a la defensa de los derechos humanos en el entorno digital. Utiliza diversas herramientas legales y de comunicación para hacer investigación de políticas, litigio estratégico, incidencia pública y campañas con el objetivo de promover los derechos digitales en México. En particular, la libertad de expresión, la privacidad, el acceso al conocimiento y la cultura libre.

Este Informe fue realizado gracias al apoyo de:

Internews
Local voices. Global change.

OPEN SOCIETY FOUNDATIONS

PRIVACY INTERNATIONAL

La información y opiniones vertidas no reflejan necesariamente los criterios o visiones institucionales de estas organizaciones

Noviembre de 2016

Diseño: Citlalli Dunne

ÍNDICE

1 INTRODUCCIÓN

El creciente uso de tecnologías digitales por parte de la ciudadanía, en particular de teléfonos móviles, ha provocado un gran interés en las autoridades por adquirir capacidades legales y tecnológicas para acceder a la gran cantidad de datos que el uso de dichos dispositivos arroja.

El acceso al contenido de las comunicaciones de una persona, así como el análisis de los datos de localización o el historial de comunicaciones de los usuarios de telecomunicaciones, **otorga al Estado un alto poder invasivo y control sobre la persona vigilada.**

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

La naturaleza de secrecía con que se lleva a cabo la vigilancia de las comunicaciones de las persona representa un serio desafío cuando se busca evitar y combatir el abuso de estas medidas pues es sumamente difícil detectarlos, tanto por la persona vigilada como por contrapesos institucionales, sin mecanismos de fiscalización adecuados.

Por estos motivos ha sido ampliamente reconocido que las medidas de vigilancia deben encontrarse especialmente reguladas y controladas: que las leyes que establecen medidas de vigilancia deben ser particularmente detalladas respecto de quiénes, cómo, cuándo y **con qué límites se puede emplear la vigilancia**; que es vital el **control judicial previo** o inmediato de las medidas de vigilancia; así como que deben existir mecanismos de rendición de cuentas como la **transparencia**, la **supervisión** independiente y la **notificación** diferida a los afectados.

El Estado de la Vigilancia: Fuera de Control pretende analizar y explicar la regulación y práctica de la vigilancia en México. Esto con la intención de promover, con base en evidencia, el establecimiento de controles democráticos que impida el abuso de estas medidas y su impunidad.

En un primer momento *(capítulo 2)* el informe explica **cuáles deben ser los controles democráticos que deben regular la vigilancia** de acuerdo a los estándares internacionales más protectores de derechos humanos. Posteriormente *(capítulo 3)*, se lleva a cabo el análisis respecto de la manera en la que la **legislación y su interpretación judicial** entienden y regulan la vigilancia en México. A continuación *(capítulo 4)* se exploran detalladamente los avances y retos de la transparencia respecto de la vigilancia en México. Luego *(capítulo 5)* se presentan **datos estadísticos sobre la vigilancia** en México y se analiza lo que ellos revelan. Por último *(capítulo 6)* se revelan los hallazgos respecto de la adquisición y **utilización ilegal de herramientas sofisticadas de vigilancia** por parte de autoridades mexicanas.

2 CONTROLES DEMOCRÁTICOS A LA VIGILANCIA ESTATAL

El poder altamente invasivo de la vigilancia y la dificultad de detectar abusos, como consecuencia de la secrecía con que se lleva a cabo por el Estado, exige el diseño y aplicación de diversas medidas de control y contrapesos institucionales que prevengan o remedien instancias de ejercicio abusivo de la vigilancia estatal.

El concepto de vigilancia estatal se refiere a la **recolección, almacenamiento, monitoreo y análisis de información personal llevada a cabo por parte de autoridades públicas** o por requerimiento de ellas. La vigilancia puede comprender la recolección, almacenamiento, monitoreo o análisis tanto del contenido de comunicaciones, como de otros datos relacionados con esas comunicaciones (comúnmente llamados "metadatos" o "datos de tráfico de comunicaciones"), pero también, de manera creciente, de otra información personal generada por las personas al interactuar con productos, servicios, e incluso, espacios públicos.

El conocimiento que puede desprenderse del análisis de esta información, **permite construir un perfil sumamente detallado de una persona**, lo cual representa riesgos a la privacidad, la seguridad y el patrimonio de la misma, sobre todo cuando ese conocimiento es adquirido por personas con un interés de generar ese daño o con la intención de obtener un beneficio personal, político o económico sin consideración de los efectos adversos generados en la persona vigilada.

No obstante, los riesgos de la vigilancia pueden generarse **desde la recolección de los datos**, por ejemplo, cuando se utilizan métodos que comprometen la seguridad general de un dispositivo o sistema; **o inclusive por su solo almacenamiento**, por ejemplo, por virtud de disposiciones que obligan a empresas a conservar registros de información personal con el único propósito de facilitar la vigilancia, pues la sola existencia de dichos registros, representa un riesgo de acceso ilícito que es imposible de eliminar y que con frecuencia se ha materializado.

En 2014, *The Intercept* publicó que, con base en información revelada por Edward Snowden, la Agencia de Seguridad Nacional de los Estados Unidos (NSA) accede y recolecta los metadatos de comunicaciones conservados por las empresas de telecomunicacio-

nes de México, como parte de su programa *MYSTIC*[1]. Igualmente, existen testimonios de personas que han recurrido al mercado negro para obtener datos de comunicaciones de familiares desaparecidos[2].

¿QUÉ TANTO REVELAN LOS METADATOS DE COMUNICACIONES?

Los metadatos de comunicaciones son datos sobre las comunicaciones de una persona, por ejemplo: los números telefónicos de origen y destino de una comunicación; la hora, fecha y duración de la misma; los datos de identificación de la tarjeta SIM (IMSI) y del dispositivo (IMEI); e incluso los datos de localización de las antenas a las cuáles se conecta un dispositivo móvil.

De manera frecuente se pretende minimizar cuan invasiva puede ser la recolección, almacenamiento y análisis de metadatos de comunicaciones, en particular respecto del contenido de las comunicaciones. Sin embargo, **los metadatos de comunicaciones pueden revelar tanta o mucha más información personal que el contenido mismo** de las comunicaciones.

En el año 2009, Malte Spitz, un integrante del Partido Verde Alemán, **demandó a la empresa de telecomunicaciones T-Mobile para acceder a sus metadatos** de comunicaciones y, una vez obtenidos, publicó una visualización interactiva de los mismos en la página de Internet del semanario alemán *Die Zeit*[3]. Del análisis de los metadatos, en conjunto con otra información públicamente disponible, se desprenden patrones de movimiento y comunicaciones que, por ejemplo, permiten conocer los lugares en los que Spitz durmió o las personas con las que frecuenta tener comunicaciones, así como sus actividades políticas.

En 2014, investigadores de la Universidad de Stanford[4] analizaron los metadatos de comunicaciones de 546 voluntarios y lograron conocer datos altamente sensibles sobre las personas. Por ejemplo, un voluntario se comunicó con varios grupos sobre neurología, una farmacia especializada, un servicio de atención a condiciones raras y

[1.] The Intercept. *Data Pirates of the Caribbean.* 19 de mayo de 2014. Disponible en: ***https://theintercept.com/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/***

[2.] NTR. *Niegan datos a familias de desaparecidos.* 29 de febrero de 2016. Disponible en: ***http://www.ntrguadalajara.com/post.php?id_nota=31771***

[3.] Zeit Online. *Tell-all telephone.* 10 de marzo de 2011. Disponible en: ***http://www.zeit.de/datenschutz/malte-spitz-data-retention***

[4.] Jonathan Mayer y Patrick Mutchler. *Metaphone: The Sensitivity of Telephone Metadata.* 12 de marzo de 2014. Disponible en: ***http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/***

a un número directo de una farmacia utilizado exclusivamente por pacientes de esclerosis múltiple, lo cual llevó a los investigadores a deducir que el voluntario padecía dicha enfermedad. Los investigadores corroboraron el análisis después de contactar al voluntario. De igual manera, el análisis de los metadatos le permitió a los investigadores deducir un posible aborto, la posesión de un arma de asalto, enfermedades y otras cuestiones altamente sensibles.

La evidencia científica es clara. Los metadatos de comunicaciones son datos personales sensibles. Por ello, la regulación de la recolección y análisis de los metadatos de comunicaciones, y en general, de los metadatos que las personas generamos al interactuar con servicios, comercios, personas y lugares, debe contemplar los riesgos que representa la vigilancia respecto de estos datos para la privacidad, la seguridad y el ejercicio de derechos humanos de todas las personas.

En los últimos años, la jurisprudencia y doctrina emanada de órganos internacionales de protección de derechos humanos y de tribunales nacionales han desarrollado estándares de protección de los derechos humanos en el contexto de la vigilancia estatal. Otros esfuerzos de la academia y la sociedad civil han recogido y articulado esos estándares al elaborar los "Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones" [5].

Observando lo anterior, a continuación se detallan los controles democráticos que deben regular la vigilancia estatal.

2.1 LEYES CLARAS Y DETALLADAS

Las facultades de vigilancia estatal deben establecerse de manera **clara, precisa y detallada en una ley**, en el sentido formal y material. Resulta vital que la sociedad pueda conocer de antemano los casos y circunstancias en los que podría ser vigilada, así como identificar las autoridades, los límites y los procedimientos que deben respetarse para prevenir o evitar abusos.

La importancia de la existencias de una base legal clara y detallada ha sido reconocida, entre muchos otros, por 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, los cuales han señalado en la Declaración Conjunta sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión que:

[5.] *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones*, disponible en: *https://es.necessaryandproportionate.org/text*

> "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." [6]

De igual manera, tribunales internacionales en materia de derechos humanos, como el Tribunal Europeo de Derechos Humanos (TED) han señalado que en el contexto de medidas de vigilancia encubierta, 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 medida [7]. Además de señalar 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[8].

2.2 NECESIDAD Y PROPORCIONALIDAD

En un Estado democrático de derecho, no cualquier medida que sea útil para alcanzar un objetivo legítimo del Estado puede considerarse, por ese solo hecho, una medida legítima. En este sentido, para que una medida de vigilancia pueda ser considerada compatible con las normas de derechos humanos, no basta con que el Estado señale que la misma persigue un fin legítimo. Es necesario que la medida de vigilancia sea, además, necesaria y proporcional.

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[9], y **proporcional**, si la afectación al derecho humano no resulta exagerada o desmedida frente a las ventajas que se obtienen mediante tal limitación [10].

[6.] *Declaración Conjunta sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión* del 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. 2013, párr. 8.

[7.] 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.

[8.] TEDH. Caso de Uzun vs. Alemania. Aplicación No. 35623/05. Sentencia de 2 de septiembre de 2010, párr. 61; Weber y Sarabia vs. Alemania. Aplicación No. 54934/00. Decisión de 29 de Junio de 2006. párr. 93.

[9.] Corte IDH. *Caso Kimel vs. Argentina.* Sentencia de 2 de mayo de 2008. Serie C No. 177. Párrafo 74.

[10.] Corte IDH. *Caso Kimel vs. Argentina.* Sentencia de 2 de mayo de 2008. Serie C No. 177. Párrafo 83.

En atención a 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 por la vigilancia.

Lo anterior implica que, por constituir una afectación indiscriminada de los derechos de una cantidad enorme de persona, **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. [11]

Igualmente, los principios de necesidad y proporcionalidad implican que los métodos a través de los cuales se lleve a cabo la vigilancia deben ser cuidadosos de no comprometer la seguridad y privacidad de manera generalizada. En este sentido, no es legítimo exigir a proveedores de servicios o fabricantes de tecnología que, de manera intencional, diseñen e implementen vulnerabilidades en sus productos con el objetivo de facilitar la vigilancia estatal.

Por ejemplo, **no es legítimo exigir el establecimiento de *"puertas traseras" (backdoors)* o exigir el debilitamiento de los estándares de cifrado en servicios, sistemas y productos** [12], pues dichas medidas, al comprometer gravemente la seguridad, privacidad y patrimonio de todos los usuarios de esos servicios y productos, son claramente desproporcionadas.

Asimismo, el Estado, al adquirir conocimiento sobre una vulnerabilidad en un servicio o producto no conocida anteriormente ("vulnerabilidad de día cero" o "zero-day vulnerability"), debe iniciar un proceso de revelación responsable de dicha vulnerabilidad al encargado de la prestación del servicio o del diseño, fabricación o comercialización del sistema o producto, de manera que dicha vulnerabilidad sea remediada a la brevedad posible y se proteja así la seguridad y privacidad de los usuarios.

No es legítimo que el Estado aproveche o almacene una vulnerabilidad para uso futuro con propósitos de vigilancia. Esta práctica puede tener consecuencias catastróficas para la privacidad y seguridad de millones de personas. Por ejemplo, en 2016 fue revelado que un grupo autodenominado *Shadow Brokers* publicó y subastó decenas de vulnerabilidades respecto de las cuales existen fuertes indicios de que fueron robadas a la Agencia de Seguridad Nacional de los Estados Unidos (NSA) [13]. De confirmarse

[11.] Ver 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. Párrafo 62.

[12.] ONU. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de expresión David Kaye. 22 de mayo de 2015. A/HRC/29/32.

[13.] WIRED. *The Shadow Brokers mess is what happens when the NSA hoards zero-days.* 17 de agosto de 2016. Disponible en: https://www.wired.com/2016/08/shadow-brokers-mess-happens-nsa-hoards-zero-days/

esta información, la seguridad y privacidad de millones de sistemas, equipos y personas habrían estado expuestos a ataques por parte de personas desconocidas. Ataques que podrían haber sido prevenidos, si la NSA hubiera iniciado procedimientos de revelación responsable de esas vulnerabilidades.

Igualmente, **el uso de software malicioso *(malware)***, que usualmente explota vulnerabilidades desconocidas en un servicio o producto para infectar a un objetivo con un programa que permita la vigilancia, **no constituye, en principio, un método legítimo para interferir en la privacidad de las personas.**

Por un lado, se han documentado formas de software malicioso que otorgan capacidades inusitadas de control sobre un sistema o dispositivo como la recolección de datos en el disco duro, el registro de todo lo tecleado *(keylogger)*, la activación subrepticia del micrófono o la cámara del dispositivo o hasta la implantación de archivos [14]. Pero además, la ausencia de la necesidad de colaboración por parte de un tercero, aunada a que este tipo de ataques resultan ser particularmente difíciles de detectar técnicamente, implica un riesgo de abuso agravado que no puede ser desestimado.

Es por ello que únicamente bajo circunstancias extremas, en las que otros métodos menos invasivos de vigilancia no sean efectivos, y sólamente bajo un régimen especialmente estricto de control judicial y supervisión independiente, podría considerarse justificado el uso de software malicioso por parte del Estado.

2.3 CONTROL JUDICIAL

A diferencia de otro tipo de interferencias en el ejercicio de derechos, la interferencia en el derecho a la privacidad que supone la vigilancia, normalmente es desconocida por las personas vigiladas. Lo anterior, impide a las personas afectadas resistir legalmente la intromisión en caso de considerarla inadecuada o abusiva. Es por ello que la presencia de un tercero que controle y supervise la vigilancia, es **vital para evitar o remediar los riesgos de abuso** que la naturaleza secreta de la vigilancia irremediablemente produce.

Típicamente se ha reconocido que esa función de control le corresponde a una autoridad judicial, la cual debe **ponderar, de manera previa o inmediata, la legitimidad de cualquier medida de vigilancia** encubierta y su estricto apego a la ley y a los principios de finalidad legítima, idoneidad, necesidad y proporcionalidad.

En este sentido la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos ha señalado que:

[14.] Para un análisis más detallado, ver el Capítulo 6 de este Informe.

> "Las decisiones de realizar tareas de vigilancia que invadan la privacidad de las personas deben ser autorizadas por autoridades judiciales independientes, que deben dar cuenta de las razones por las cuales la medida es idónea para alcanzar los fines que persigue en el caso concreto; de si es lo suficientemente restringida para no afectar el derecho involucrado más de lo necesario; y de si resulta proporcional respecto del interés que se quiere promover." [15]

En algunas ocasiones, se ha invocado la necesidad de celeridad en una investigación para intentar justificar la ausencia del requisito de autorización judicial para ciertas medidas de vigilancia. Sin embargo, existen diseños normativos e institucionales en los que no es necesario prescindir del control judicial para que, en casos de emergencia, las autoridades competentes puedan llevar a cabo medidas de vigilancia de manera inmediata.

Como lo señalan los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones[16] y como se reconoce en diversas jurisdicciones [17], es posible establecer un mecanismo de emergencia en el que, por ejemplo, una autoridad pueda llevar a cabo una medida de vigilancia de manera inmediata, siempre y cuando se solicite la autorización judicial de manera simultánea. De esta manera, la autorización judicial posterior tendría efectos retroactivos, o en su defecto, la negativa de dicha autorización debería conducir a la subsanación de los defectos de la solicitud o a la destrucción de los datos obtenidos y, en su caso, la imposición de sanciones por la utilización abusiva del mecanismo de emergencia.

FISCALIZACIÓN Y RENDICIÓN DE CUENTAS

Organismos de protección internacional de derechos humanos como el Tribunal Europeo de Derechos Humanos [18], la Asamblea General de la Organización de las Naciones Unidas (ONU) [19], el Relator Especial de la ONU para el Derecho a la Libertad de Expresión y Opinión [20], la Alta Comisionada para los Derechos Humanos de la ONU [21],

[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/necesarios-proporcionados

[17.] Ver, por ejemplo, la Electronic Communications Privacy Act de los Estados Unidos.

[18.] 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.

[19.] 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.

[20.] 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.

[21.] OACNUDH. El derecho a la privacidad en la era digital. 30 de junio de 2014. A/HRC/27/37.

la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana sobre Derechos Humanos [22], así como los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones [23] coinciden en la necesidad del establecimiento de diversas salvaguardas para inhibir los riesgos de abuso de la vigilancia, además del control judicial.

En la resolución "El derecho a la privacidad en la era digital", adoptada por consenso por los miembros de la Asamblea General de la ONU el 18 de diciembre de 2013, 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" [24].

Además de las **obligaciones de transparencia**, que se analizan de manera detallada en el capítulo 4 de este Informe, se ha reconocido la importancia del establecimiento de mecanismos de supervisión independiente, así como la garantía del derecho de notificación al afectado.

Como ha sido reconocido por el Principio 10 de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones [25], es necesario que se establezca un **mecanismo de supervisión independiente de las medidas de vigilancia.**

El mecanismo de supervisión independiente debe tener facultades de acceso a toda la información necesaria para fiscalizar la utilización de medidas de vigilancia, incluyendo aquella de carácter confidencial o reservada. Además, debe tener la capacidad de producir informes públicos, recomendaciones e incluso presentar denuncias o llevar a cabo investigaciones sobre instancias en las que se detecte un ejercicio abusivo de medidas de vigilancia.

A nivel internacional existen algunos ejemplos de este tipo de mecanismos como es el caso del Reino Unido donde, aunque posee facultades limitadas, existe un "Comisionado de Interceptación de Comunicaciones" [26].

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

[23.] Análisis Jurídico Internacional de Apoyo y Antecedentes de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: *https://es.necessaryandproportionate.org/AnalisisLegal*

[24.] 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.

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

[26.] Interception of Communications Commissioner's Office. Disponible en: *http://www.iocco-uk.info/sections.asp?sectionID=2&type=top*

Otra de las salvaguardas para garantizar la necesidad y proporcionalidad de las medidas de vigilancia es el **derecho de notificación al afectado**. Este derecho de notificación a las personas afectadas por medidas de vigilancia ha sido reconocido por diversas instancias incluyendo al Relator Especial sobre el derecho a la libertad de opinión y expresión de la Organización de las Naciones Unidas:

> "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" [27]

Este derecho de notificación ha sido reconocido también por el Tribunal Europeo de Derechos Humanos, el cual determinó en el Caso *Ekimdzhiev 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 lo más pronto posible** [28]**.**

De esta manera, el derecho de notificación diferida permite que las personas puedan conocer en algún momento que fueron vigiladas y, en su caso, **acudir a los mecanismos jurídicos que considere pertinentes para remediar posibles abusos** sin que se obstaculice de forma alguna la actividad legítima de alguna autoridad.

[27.] 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

[28.] 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.

3 LA VIGILANCIA Y LA LEY EN MÉXICO

En años recientes, México ha adoptado legislación para expandir las facultades legales de llevar a cabo medidas de vigilancia. De igual manera, el Poder Judicial de la Federación ha tenido la oportunidad de interpretar el derecho a la privacidad en el contexto de la vigilancia.

En 2014, ante la incorporación de medidas de vigilancia dentro de la Ley Federal de Telecomunicaciones y Radiodifusión con un lenguaje vago e impreciso, R3D interpuso un juicio de amparo el cual otorgó a la Suprema Corte de Justicia de la Nación la oportunidad de analizar y clarificar el contenido y alcance del derecho a la privacidad ante medidas de vigilancia de comunicaciones.

En este capítulo se explicarán, de manera resumida, los aspectos más relevantes de la regulación y la interpretación judicial relacionada con medidas de vigilancia en México [29].

3.1 ¿QUÉ FORMAS DE VIGILANCIA RECONOCE LA LEY?

Las medidas de vigilancia se encuentran dispersas en diversas leyes y su formulación y lenguaje son usualmente vagos e imprecisos. No obstante, es posible identificar patrones y prácticas comunes.

3.1.1 CONSERVACIÓN OBLIGATORIA DE METADATOS DE COMUNICACIONES

El artículo 190 fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR) obliga a las empresas que prestan servicios de telecomunicaciones a conservar por 24 meses una serie de datos de comunicaciones comúnmente conocidos como "metadatos de comunicaciones" o "datos de tráfico de comunicaciones" dentro de lo que la ley llama "Registro de Comunicaciones". Como parte de los datos que deben conservarse se encuentran:

[29.] Para un análisis detallado, consultar R3D y EFF. Vigilancia Estatal de Comunicaciones y Protección de los *Derechos Fundamentales en México*. Agosto de 2016. Disponible en: ***https://necessaryandproportionate.org/es/country-reports/mexico***

- Nombre, denominación o razón social y domicilio del suscriptor;
- **Tipo de comunicación** (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluidos el reenvío o transferencia de llamada) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia y avanzados);
- Datos necesarios para **rastrear e identificar el origen y destino de las comunicaciones** de telefonía móvil: número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas de prepago;
- Datos necesarios para determinar la fecha, hora y duración de la comunicación, así como el servicio de mensajería o multimedia;
- Además de los datos anteriores, se deberá conservar la fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda) desde la que se haya activado el servicio;
- En su caso, identificación y características técnicas de los dispositivos, incluyendo, entre otros, los códigos internacionales de identidad de fabricación del equipo y del suscriptor;
- La **ubicación digital del posicionamiento geográfico** de las líneas telefónicas.

Este tipo de obligaciones de **conservación obligatoria de datos ha sido rechazada por organismos internacionales de protección de derechos humanos** como el Relator Especial sobre la promoción y protección del derecho a la libertad de expresión de la ONU [30] y por tribunales como el Tribunal de Justicia de la Unión Europea [31], en tanto este tipo de registros constituyen una interferencia masiva e indiscriminada en la privacidad de millones de personas, lo cual no se adecúa a los principios de necesidad y proporcionalidad.

Sin embargo, la Suprema Corte de Justicia de la Nación, al resolver el amparo en revisión 964/2015 interpuesto por R3D, decidió validar la constitucionalidad del registro de comunicaciones[32], sin siquiera reconocer que la conservación masiva y prolongada de datos, más allá de lo necesario para la prestación del servicio, constituye una interferencia con el derecho a la privacidad y sin analizar la necesidad y proporcionalidad de la misma.

[30.] 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, Párrafo 15.

[31.] Tribunal de Justicia de la Unión Europea. *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. Disponible en: ***http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0293&lang1=es&type=TXT&ancre=***

[32.] SCJN. Segunda Sala. *Amparo en Revisión 964/2015*. Sentencia de 4 de mayo de 2016.

3.1.2 INTERVENCIÓN DE COMUNICACIONES PRIVADAS (INCLUYENDO EL ACCESO A METADATOS DE COMUNICACIONES)

El artículo 16 de la Constitución Política de los Estados Unidos (en adelante "la Constitución") reconoce y limita la posibilidad de llevar a cabo la intervención de comunicaciones privadas. Esta posibilidad se contempla, a su vez, en diversas leyes federales.

El artículo 291 del Código Nacional de Procedimientos Penales define la intervención de comunicaciones privadas 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 esta manera, esta y otras leyes entienden que la intervención de comunicaciones privadas no se refiere únicamente al conocimiento del contenido de una comunicación, sino que también comprende los "metadatos de comunicaciones".

Otras leyes que contemplan la intervención de comunicaciones privadas son:

- Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro (Art. 24)[33]
- Ley Federal contra la Delincuencia Organizada (Arts. 15 - 28) [34]
- Ley de la Policía Federal (Arts. 48 - 55) [35]
- Ley de Seguridad Nacional (Arts. 33 - 49) [36]
- Código Militar de Procedimientos Penales (Art. 287) [37]
- Ley Federal de Telecomunicaciones y Radiodifusión(Art. 190, fracción II y III - *acceso al registro de comunicaciones*) [38]
- Lineamientos de Colaboración en Materia de Seguridad y Justicia del Instituto Federal de Telecomunicaciones (IFT) [39]

[33.] Disponible en: ***http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPSDMS_170616.pdf***
[34.] Disponible en: ***http://www.diputados.gob.mx/LeyesBiblio/pdf/101_160616.pdf***
[35.] Disponible en: ***http://www.diputados.gob.mx/LeyesBiblio/pdf/LPF.pdf***
[36.] Disponible en: ***http://www.diputados.gob.mx/LeyesBiblio/pdf/LSegNac.pdf***
[37.] Disponible en: ***http://www.diputados.gob.mx/LeyesBiblio/pdf/CMPP.pdf***
[38.] Disponible en: ***http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR_090616.pdf***
[39.] Disponible en: ***http://dof.gob.mx/nota_detalle.php?codigo=5418339&fecha=02/12/2015***

3.1.3 GEOLOCALIZACIÓN EN TIEMPO REAL

La legislación mexicana también contempla la facultad de requerir a empresas que prestan servicios de telecomunicaciones, la localización geográfica, en tiempo real, de equipos de comunicación móvil.

Esta facultad se encuentra regulada en el artículo 190, fracción I, de la Ley Federal de Telecomunicaciones y Radiodifusión, así como en el artículo 303 del Código Nacional de Procedimientos Penales y en el Capítulo III de los Lineamientos de Colaboración en Materia de Seguridad y Justicia del Instituto Federal de Telecomunicaciones (IFT).

3.2 ¿QUIÉN PUEDE LLEVAR A CABO MEDIDAS DE VIGILANCIA?

La vaguedad e imprecisión de las leyes que contemplan medidas de vigilancia ha dado pie a diversas interpretaciones en torno a cuáles autoridades poseen facultades de vigilancia.

El artículo 16 constitucional, sin embargo, limita el universo de autoridades competentes de manera considerable. El párrafo decimosegundo del artículo 16 establece dos categorías de autoridades susceptibles contar con autorización constitucional para intervenir comunicaciones privadas: (i) autoridades federales facultadas por una ley y (ii) el titular del Ministerio Público de las entidades federativas.

En la interpretación de este precepto dentro del Amparo en Revisión 964/2015 anteriormente mencionado la SCJN ha clarificado que, del análisis de la legislación vigente, únicamente pueden considerarse facultadas para intervenir comunicaciones privadas, incluyendo el acceso al registro de comunicaciones, así como para llevar a cabo la geolocalización en tiempo real, a las siguientes autoridades [40]:

1. El o la titular de la **Procuraduría General de la República**, así como las y los procuradores de las entidades federativas.

2. La **Policía Federal.**

3. El **Centro de Investigación y Seguridad Nacional (CISEN).**

De esta manera, cualquier autoridad distinta a las anteriormente mencionadas se encuentra impedida legalmente para llevar a cabo medidas de vigilancia.

[40.] SCJN. Segunda Sala. *Amparo en Revisión 964/2015*. Sentencia de 4 de mayo de 2016. Páginas 62-63.

3.3 ¿CUÁNDO Y CÓMO PUEDE EMPLEARSE LA VIGILANCIA?

El artículo 16 constitucional exige que toda intervención de comunicaciones privadas debe contar con una autorización judicial federal previa. La SCJN, al interpretar dicho artículo en el Amparo en Revisión 964/2015, concluyó que las autoridades que pretendan llevar a cabo medidas de vigilancia de comunicaciones, deben cumplir el requisito de autorización judicial federal previa tanto para la vigilancia del contenido de comunicaciones, como de los "metadatos de comunicaciones".

De esta forma, toda intervención de comunicaciones privadas, incluyendo el acceso al "Registro de Comunicaciones" **requiere una autorización judicial federal previa** [41].

El artículo 16 constitucional y la legislación que regula las medidas de vigilancia exige que las solicitudes de autorización judicial señalen con claridad los fundamentos legales, el tipo de intervención, los sujetos de la misma y su duración.

Además, la Constitución limita las materias en las que la autoridad judicial federal puede otorgar la autorización de una medida de vigilancia de comunicaciones. En concreto **se prohíbe la intervención de comunicaciones privadas cuando se trate de cuestiones de carácter electoral, fiscal, mercantil, civil, laboral o administrativo**, ni en el caso de las comunicaciones del detenido con su defensor.

Por otro lado, la SCJN ha interpretado que el requisito de autorización judicial no resulta necesario constitucionalmente cuando se trate del monitoreo de la localización geográfica, en tiempo real, de equipos de comunicación móvil [42]. Lo anterior resultaría contradictorio, en tanto que, bajo el parámetro establecido por la SCJN, es necesaria una autorización judicial para conocer datos de localización histórica de un usuario de telecomunicaciones conservados dentro del "Registro de Comunicaciones", pero no resultaría necesaria la autorización judicial para monitorear la localización en tiempo real, cuando probablemente el poder invasivo de la medida es mayor.

No obstante lo anterior, el artículo 303 del Código Nacional de Procedimientos Penales fue reformado en junio de 2016 para incorporar el requisito de autorización judicial previa a la geolocalización en tiempo real. Únicamente se permite llevar a cabo la medida sin autorización en casos en los que esté en peligro la integridad física o la vida de una persona, se encuentre en riesgo el objeto del delito o en hechos relacionados con delitos como el de privación ilegal de la libertad, secuestro, extorsión o delincuencia organizada. Sin embargo, la autoridad que utilice este mecanismo de emergencia debe avisar al juez de control, dentro de las 48 horas siguientes, el cual debe verificar la legalidad de la medida de vigilancia.

[41.] SCJN. Segunda Sala. *Amparo en Revisión 964/2015*. Sentencia de 4 de mayo de 2016. Páginas 80-81.
[42.] SCJN. Segunda Sala. *Amparo en Revisión 964/2015*. Sentencia de 4 de mayo de 2016. Página 67.

Tomando en cuenta las reglas generales descritas, la legislación detalla, en algunos casos, las circunstancias en las que pueden utilizarse las medidas de vigilancia:

1. **Procuraduría General de la República y Procuradurías de las entidades federativas:** El Código Nacional de Procedimientos Penales contempla la intervención de comunicaciones privadas en casos en los que le Ministerio Público lo considere **necesario para la investigación de algún delito**. Los artículos 292 a 302 detallan el procedimiento a seguir, incluyendo los requisitos y plazos de la solicitud de autorización judicial. Adicionalmente, la Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro y la Ley contra la Delincuencia Organizada, regulan en términos similares la intervención de comunicaciones privadas para la investigación de algunos delitos en específico.

2. **Policía Federal**: La Ley de la Policía Federal establece, en su artículo 48, que la intervención de comunicaciones privadas únicamente puede autorizarse cuando "**se constate la existencia de indicios suficientes que acrediten que se está organizando" la comisión de una ciertos delitos** definidos en la ley. El procedimiento de solicitud de autorización se regula de manera específica en los artículos 48 a 55.

3. **Centro de Investigación y Seguridad Nacional (CISEN):** La Ley de Seguridad Nacional establece, en el artículo 33 y siguientes, que la intervención de comunicaciones privadas **únicamente puede solicitarse en casos de amenaza a la seguridad nacional** detallados en el artículo 5 de la ley. Dicho artículo define de manera vaga e imprecisa las circunstancias en las que se considera que existe una amenaza a la seguridad nacional, sin embargo, los artículos 33 a 49 detallan el procedimiento de autorización judicial.

Además de lo anterior, el procedimiento y solicitud de acceso a los "metadatos de comunicaciones" conservados en el "Registro de Comunicaciones" que establece el artículo 190, fracción II, también se encuentra regulado en los Lineamientos sobre la colaboración en materia de seguridad y justicia del IFT.

En el caso de la localización geográfica, en tiempo real, de equipos de comunicación móvil, la ley no define de manera clara los casos y circunstancias especiales en las que esta puede llevarse a cabo, sin embargo, la SCJN, al resolver el Amparo en Revisión 964/2015, además de limitar las autoridades que pueden llevar a cabo esta medida, también señaló que ésta **únicamente puede utilizarse "cuando se presuma que existe un peligro para la vida o integridad de una persona"** [43].

[43.] SCJN. Segunda Sala. *Amparo en Revisión 964/2015*. Sentencia de 4 de mayo de 2016. Página 64-65.

3.4 ¿QUIÉN VIGILA AL VIGILANTE?

Además del control judicial establecido para algunas medidas de vigilancia, la legislación contempla pocas salvaguardas adicionales contra los riesgos de abuso.

La Ley General de Transparencia y Acceso a la Información y los Lineamientos sobre colaboración en materia de seguridad y justicia del IFT contemplan diversas obligaciones de transparencia. En el capítulo siguiente se realiza un análisis detallado de las mismas.

Por otro lado, la legislación mexicana no contempla mecanismos de supervisión independiente, ni reconoce el derecho de notificación de las personas afectadas por una medida de vigilancia.

Algunas leyes contemplan sanciones relacionadas con el abuso de medidas de vigilancia, sin embargo, al no existir salvaguardas suficientes para detectar esas instancias de abuso, resulta sumamente improbable que dichas sanciones sean efectivamente impuestas.

3.5 INCOMPATIBILIDADES CON LOS DERECHOS HUMANOS

A pesar de algunos avances normativos e interpretativos, en especial los conseguidos producto del Juicio de Amparo interpuesto por R3D en contra de la Ley Federal de Telecomunicaciones y Radiodifusión, persisten graves deficiencias en la regulación e interpretación de las facultades de vigilancia en México, en violación de los estándares y normas de derechos humanos.

Por un lado, la validación constitucional de una medida de vigilancia masiva, como lo es la obligación de conservación masiva e indiscriminada de metadatos de comunicaciones establecida en el artículo 190, fracción II de la LFTR, vulnera de manera grave la privacidad de todas las personas usuarias de telecomunicaciones del país.

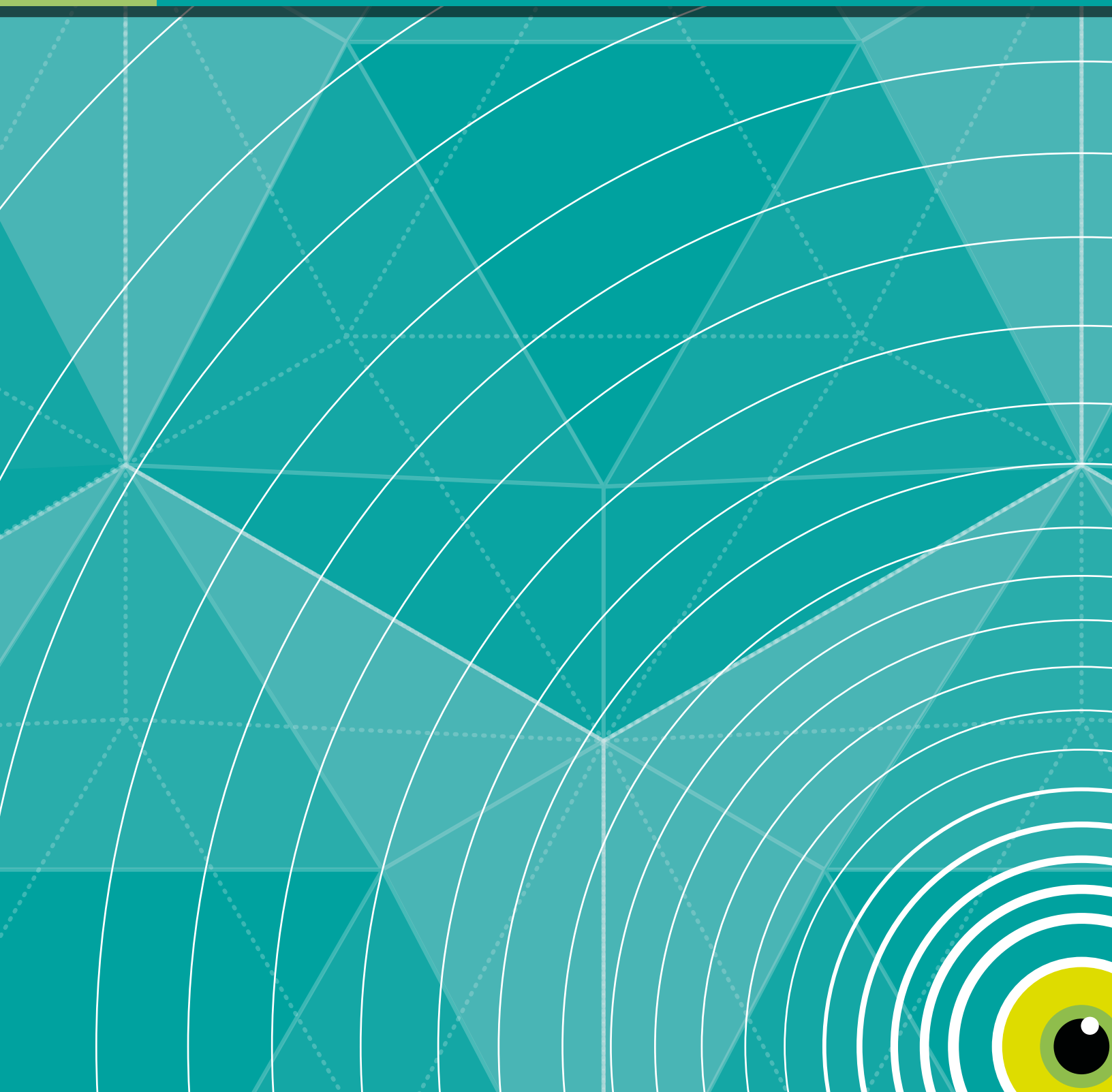
De igual manera, a pesar de que la ley ya exige la autorización judicial previa para llevar a cabo la localización geográfica, en tiempo real, de equipos de comunicación móvil, el criterio establecido por la SCJN relativo a que no sería necesaria dicha autorización judicial compromete la privacidad y seguridad de las personas, pues abre un campo para el abuso impune de dicha medida.

Respecto de estas dos graves decisiones **R3D interpondrá una petición ante la Comisión Interamericana de Derechos Humanos,** en tanto las mismas resultan incompatibles con el artículo 11 de la Convención Americana de Derechos Humanos.

Por otro lado, persisten vaguedades y omisiones en la regulación de medidas de vigilancia. Por ejemplo, persisten vaguedades respecto de los casos y circunstancias en los que ciertas autoridades pueden utilizar medidas de vigilancia, especialmente en el caso del CISEN.

Asimismo, la ausencia de salvaguardas adecuadas contra el abuso como la ausencia de un mecanismo de supervisión independiente y la falta de reconocimiento del derecho de notificación de personas afectadas por medidas de vigilancia representa un urgente pendiente regulatorio que debe R3D continuará impulsando por su incorporación.

4 TRANSPARENCIA Y VIGILANCIA EN MÉXICO



4.1 LA TRANSPARENCIA COMO MEDIO DE CONTROL DE LA VIGILANCIA

Uno de los controles democráticos indispensables para que la ciudadanía pueda ejercer un control democrático sobre la vigilancia llevada a cabo por el Estado es la transparencia.

Si bien las medidas de transparencia por sí mismas no inhiben todos los riesgos de abuso, el conocimiento de estadísticas y otras particularidades respecto de cómo es que el Estado hace uso de las medidas de vigilancia, permite a la ciudadanía conocer el volumen y alcance de estas medidas y permite informar la discusión pública sobre la pertinencia y las condiciones que deben establecerse para permitir este tipo de invasiones a la privacidad.

Con la convicción de que la transparencia, entre otras medidas, son indispensables para ejercer un control democrático sobre las autoridades que llevan a cabo medidas de vigilancia, R3D ha promovido la inclusión de obligaciones de transparencia en distintos procesos normativos, tanto legales como regulatorios. Asimismo, ha puesto a prueba las herramientas legales para el acceso a la información y promovido la adopción de interpretaciones y decisiones administrativas y judiciales que sienten un precedente de rendición de cuentas frente a la vigilancia estatal.

4.2 TRANSPARENCIA Y VIGILANCIA EN INSTRUMENTOS INTERNACIONALES

La importancia de la transparencia respecto de la vigilancia estatal ha sido reconocida por organismos de protección internacional de derechos humanos e incluso por el propio gobierno Mexicano ante organismos multilaterales. Por ejemplo, en la resolución "El derecho a la privacidad en la era digital" adoptada por consenso por los miembros de la Asamblea General de la ONU el 18 de diciembre de 2013 y, de nuevo, el 19 de noviembre de 2014, ambas promovidas por el gobierno Mexicano, 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" [44].

Por su parte, el Relator Especial sobre el derecho a la libertad de opinión y expresión de la Organización de las Naciones Unidas (ONU) ha expresado en su Informe las consecuencias de la vigilancia de las comunicaciones que:

> "Los Estados deben ser **completamente transparentes respecto del uso y alcance de los poderes y técnicas de vigilancia de las comunicaciones.** De-

[44.] 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.

> ben 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. (...)**" [45]

De igual manera en la Declaración Conjunta sobre Programas de Vigilancia y su Impacto para la Libertad de Expresión [46] del Relator Especial sobre el derecho a la libertad de opinión y expresión de la ONU y la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana sobre Derechos Humanos (CIDH) han señalado que:

> **"Toda persona tiene derecho a acceder a información bajo el control del Estado**. Este derecho incluye la información que se relaciona con la seguridad nacional, salvo las precisas excepciones que establezca la ley, siempre que estas resulten necesarias en una sociedad democrática. Las leyes deben asegurar que el público pueda acceder a información sobre los programas de vigilancia de comunicaciones privadas, su alcance y los controles existentes para garantizar que no puedan ser usados de manera arbitraria. En consecuencia, los Estados deben difundir, por lo menos, información relativa al marco regulatorio de los programas de vigilancia; los órganos encargados para implementar y supervisar dichos programas; los procedimientos de autorización, de selección de objetivos y de manejo de datos, así como información sobre el uso de estas técnicas, incluidos datos agregados sobre su alcance. **En todo caso, los Estados deben establecer mecanismos de control independientes capaces de asegurar transparencia y rendición de cuentas sobre estos programas** (...)
>
> El Estado tiene la obligación de divulgar ampliamente la información sobre programas ilegales de vigilancia de comunicaciones privadas. Esta obligación debe ser satisfecha sin perjuicio del derecho a la información

[45.] 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. Disponible en inglés en: ***http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf***

[46.] 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***

> personal de quienes habrían sido afectados. En todo caso, los Estados deben adelantar investigaciones exhaustivas para identificar y sancionar a los responsables de este tipo de prácticas e informar oportunamente a quienes han podido ser víctima de las mismas."

Lo anterior ha sido reiterado por la Relatora Especial para la Libertad de Expresión de la CIDH la cual señaló en su "Informe sobre Libertad de Expresión e Internet" [47] que:

> "Los Estados **deberían publicar información global sobre el número de solicitudes de intercepción y vigilancia aprobadas y rechazadas, incluyendo la mayor cantidad de información posible** como – por ejemplo – un desglose de solicitudes por proveedor de servicios, tipo de investigación, tiempo durante el cual se extienden las investigaciones, etcétera."

Otro instrumento que reconoce la obligación de los Estados de garantizar la transparencia respecto de programas de vigilancia para fines de seguridad nacional son los Principios Globales sobre Seguridad Nacional y Derecho a la Información (Principios de Tshwane) [48] los cuales señalan en su Principio 10 "Categorías de información sobre las cuales existe una fuerte presunción o un interés esencial a favor de su divulgación":

> " E. Vigilancia (1)
>
> El público debería conocer tanto las leyes y principales reglamentaciones a todas las formas de vigilancia secreta como los procedimientos relativos a la autorización de dicha vigilancia, la selección de objetivos, el uso, intercambio, almacenamiento y la destrucción y el material interceptado.
>
> *Nota: Esta información incluye: (a) las leyes que rigen todos los tipos de vigilancia, tanto abierta como encubierta, incluidas las técnicas de vigilancia indirecta como el perfilado y la búsqueda de datos, y todas las medidas de vigilancia que puedan usarse; (b) los objetivos permisibles de vigilancia; (c) el umbral de sospecha requerido para iniciar o continuar la vigilancia; (d) límites de duración de las medidas de vigilancia; (e) procedimientos para la autorización y revisión de dichas medidas; (f) los tipos de datos personal que podrán recopilarse y/o procesarse por motivos relativos a la seguridad nacional; y (g) los criterios que se aplican al uso, retención, eliminación y transferencia de dichos datos.*
>
> (2) El público también deber tener acceso a la información sobre las entidades autorizadas para llevar a cabo acciones de vigilancia, y a las estadísticas relativas al uso de dichas acciones.

[47.] CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 31 de diciembre de 2013. OEA/Ser.L/V/II. Disponible en: ***http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf***

[48.] Principios Globales sobre Seguridad Nacional y el Derecho a la Información ("Principios de Tshwane") concluidos en Tshwane, Sudáfrica y emitidos el 12 de junio de 2013. Disponible en: ***https://www.aclu.org/sites/default/files/assets/spanish-version_of_the_tshwane_principles.doc***

> Nota: Esta información incluye la identidad de cada entidad gubernamental con autoridad para llevar a cabo vigilancias específicas cada año; el número de autorizaciones para realizar vigilancias otorgadas cada año a dichas entidades; la mejor información disponible sobre el número de individuos y el número de comunicaciones sujetos a vigilancia cada año; y si se llevaron a cabo acciones de vigilancia sin autorización específica, y si es así, por parte de qué entidad.
>
> El derecho del público a la información no se extiende, necesariamente, a los detalles fácticos u operativos de las vigilancias con arreglo a la ley y en consonancia con las obligaciones relativas a los derechos humanos. Dicha información podría ser confidencial, tanto para el público como para el objeto de la vigilancia hasta que finalicen las acciones.
>
> (3) Se debería informar al público, además, de las vigilancias ilegales. La información acerca de este tipo de vigilancias debería ser hecha pública en la mayor medida posible, sin violar los derechos de privacidad de las personas vigiladas.
>
> (4) Estos Principios abordan el derecho del público a acceder a la información y se entienden sin perjuicio a los derechos sustantivos y procesales adicionales de los individuos que han sido, o creen haber sido, sujetos a vigilancia.
>
> Nota: Se considera como una buena práctica el que se solicite a las autoridades públicas que notifiquen a las personas que han sido sujetas a vigilancia encubierta (facilitando, como mínimo, información sobre el tipo de medida que se tomó, y el órgano responsable de autorizar la medida de vigilancia) en la medida de lo posible, ya que esto puede hacerse sin poner en peligro operaciones en marcha de fuentes y métodos."

Asimismo, con el fin de que los Estados garanticen políticas y prácticas que observen las leyes y estándares internacionales de derechos humanos relativos a la vigilancia de las comunicaciones, diferentes grupos de la sociedad civil, la industria y expertos internacionales en la materia han elaborado y promovido los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones [49] dentro de los cuales se encuentra el Principio de Transparencia:

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

TRANSPARENCIA: los Estados deben ser transparentes respecto del uso y alcance de las medidas de vigilancia de las comunicaciones que implementen, debiendo publicar, como mínimo, información comprehensiva relativa al número de solicitudes aprobadas y rechazadas, un desglose de las solicitudes por proveedor de servicios, por autoridad investigadora, el tipo de medidas utilizadas, su objetivo y el número de personas afectadas por cada una, entre otros.

4.3 TRANSPARENCIA Y VIGILANCIA EN LA NORMATIVA NACIONAL

4.3.1 LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA

El 5 de mayo de 2015 entró en vigor en México la Ley General de Transparencia y Acceso a la Información Pública (LGTA) [50], después de una intensa participación de organizaciones de la sociedad civil dentro del proceso legislativo, incluyendo a R3D, la cual contempla de forma expresa obligaciones de transparencia relacionadas con las medidas de vigilancia y obliga a la Federación y los Estados a contemplar esta obligación en las leyes de transparencia correspondientes.

El artículo 70 de la LGTA establece las obligaciones de transparencia comunes a todos los sujetos obligados, enlistando aquella información que deberán poner a disposición del público de manera actualizada. La fracción XLVII de este artículo obliga a las autoridades facultadas para llevar a cabo medidas de vigilancia como la intervención de comunicaciones [51] privadas, el acceso al registro de comunicaciones y la localización geográfica en tiempo real de equipos de comunicación, a publicar datos sobre las solicitudes que realizan:

> ***Artículo 70.***
>
> *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*

[50.] Ley General de Transparencia y Acceso a la Información Pública, publicada en el Diario Oficial de la Federación el 4 de mayo de 2015. Disponible en: ***http://inicio.ifai.org.mx/MarcoNormativoDocumentos/LGTAIP.pdf***

[51.] El artículo 190 fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión establece que los concesionarios de telecomunicaciones, y en su caso, los autorizados deberán conservar, durante 24 meses, un registro y control de comunicaciones que realicen los usuarios desde cualquier tipo de línea, de manera tal que se puedan identificar sobre todo aquellos datos relativos a nombre y domicilio del suscriptor; tipo de comunicación; origen, destino, fecha, hora y duración de las comunicaciones, y la ubicación digital del posicionamiento geográfico de las líneas telefónicas, entre otros.

> *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 […]*

El plazo para que la Federación y los estados adecuarán su legislación a lo que establece la Ley General expiró el día 5 de mayo de 2016. A pesar de que algunos Estados incumplieron el plazo, en noviembre de 2016 tanto la Ley Federal de Transparencia y Acceso a la Información Pública, como las 32 leyes de transparencia locales han adecuado su legislación de conformidad con el artículo 70 XLVII de la LGTA.

ENTIDAD FEDERATIVA	LEY EN MATERIA DE TRANSPARENCIA	FECHA DE PUBLICACIÓN EN DIARIOS OFICIALES
Aguascalientes	Ley de Transparencia y Acceso a la Información Pública del Estado de Aguascalientes y sus Municipios	07/11/2016
Baja California	Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California	29/04/2016
Baja California Sur	Ley de Transparencia y Acceso a la Información Pública del Estado de Baja California Sur	04/05/2016
Campeche	Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche	22/03/2016
Ciudad de México	Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México	06/05/2016
Chiapas	Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas	04/05/2016
Chihuahua	Ley de Transparencia y Acceso a la Información Pública del Estado de Chihuahua	29/08/2015
Coahuila	Ley de Acceso a la Información Pública y Protección de Datos Personales para el Estado de Coahuila Zaragoza	04/03/2016
Colima	Ley de Transparencia y Acceso a la Información Pública del Estado de Colima	30/05/2016
Durango	Ley de Transparencia y Acceso a la Información Pública del Estado de Durango	04/05/2016
Estado de México	Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios	04/05/2016
Guanajuato	Ley de Transparencia y Acceso a la Información Pública para el Estado y Municipios de Guanajuato	13/05/2016
Guerrero	Ley Número 207 de Transparencia y Acceso a la Información Pública del Estado de Guerrero	06/05/2016
Hidalgo	Ley de Transparencia y Acceso a la Información Pública para el Estado de Hidalgo	04/05/2016

ENTIDAD FEDERATIVA	LEY EN MATERIA DE TRANSPARENCIA	FECHA DE PUBLICACIÓN EN DIARIOS OFICIALES
Jalisco	Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios	10/11/2015
Michoacán	Ley de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Michoacán de Ocampo	18/05/2016
Morelos	Ley de Transparencia y Acceso a la Información Pública del Estado de Morelos	27/04/2016
Nayarit	Ley de Transparencia y Acceso a la Información Pública del Estado de Nayarit	03/05/2016
Nuevo León	Ley de Transparencia y Acceso a la Información Pública del Estado de Nuevo León	01/07/2016
Oaxaca	Ley de Transparencia y Acceso a la Información Pública para el Estado de Oaxaca	11/03/2016
Puebla	Ley de Transparencia y Acceso a la Información Pública del Estado de Puebla	04/05/2016
Querétaro	Ley de Transparencia y Acceso a la Información Pública del Estado de Querétaro	25/01/2016
Quintana Roo	Ley de Transparencia y Acceso a la Información Pública para el Estado de Quintana Roo	03/05/2016
San Luis Potosí	Ley de Transparencia y Acceso a la Información Pública del Estado de San Luis Potosí	09/05/2016
Sinaloa	Ley de Acceso a la Información Pública del Estado de Sinaloa	04/05/2016
Sonora	Ley de Transparencia y Acceso a la Información Pública del Estado de Sonora	28/04/16
Tabasco	Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco	15/12/15
Tamaulipas	Ley de Transparencia y Acceso a la Información Pública del Estado de Tamaulipas	27/04/2016
Tlaxcala	Ley de Transparencia y Acceso a la Información Pública del Estado de Tlaxcala	04/05/2016
Veracruz	Ley Número 875 de Transparencia y Acceso a la Información Pública para el Estado de Veracruz de Ignacio de la Llave	29/09/2016
Yucatán	Ley de Transparencia y Acceso a la Información Pública del Estado de Yucatán	02/05/2016
Zacatecas	Ley de Transparencia y Acceso a la Información Pública del Estado de Zacatecas	02/06/2016

Asimismo, de acuerdo a lo que señalan los artículos 60, 62, 64 y octavo transitorio de la Ley General, la información estadística sobre medidas de vigilancia debe ser publicada proactivamente en los sitios de Internet de cada autoridad y en la Plataforma Nacional de Transparencia (PNT) y debe ser actualizada, por lo menos, cada tres meses.

De conformidad con los Lineamientos Técnicos Generales para la publicación de la información que deben difundir los sujetos obligados en los portales de Internet y en la PNT emitidos por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) [52], el plazo para que las obligaciones de transparencia proactiva iniciaran a cumplirse concluía a inicios de noviembre de 2016, sin embargo, mediante un acuerdo publicado el 2 de noviembre de 2016, se amplió el plazo hasta el 4 de mayo de 2017[53].

Los Lineamientos establecen con mayor detalle la información que los sujetos obligados deberán publicar. Por ejemplo, respecto de la solicitudes de intervención de comunicaciones privadas deberá publicarse:

- Ejercicio (año)
- Periodo que se informa (enero-marzo, abril-junio, julio-septiembre, octubre-diciembre)
- Fundamento legal del requerimiento: artículo, fracción, inciso
- Alcance temporal
- Por cada solicitud, indicar si hubo autorización judicial: (Sí/No)
- Denominación de la empresa concesionaria de los servicios de comunicación vía satélite o telecomunicaciones que colaboraron en el proceso de intervención
- Número total de solicitudes de intervención realizadas

Respecto de las solicitudes de acceso al registro de comunicaciones y solicitud de localización geográfica, los sujetos obligados deben especificar los siguientes datos en su informe semestral:

[52.] 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 difundir los sujetos obligados en los portales de Internet y en la Plataforma Nacional de Transparencia, publicados en el Diario Oficial de la Federación el 04 de mayo de 2016. Disponible en: ***http://www.dof.gob.mx/nota_detalle.php?codigo=5436072&fecha=04/05/2016***

[53.] Acuerdo por el cual se aprueba la modificación del plazo para que los sujetos obligados de los ámbitos Federal, Estatal y Municipal incorporen a sus portales de Internet y a la Plataforma Nacional de Transparencia, la información a la que se refieren el Título Quinto y la Fracción IV del artículo 31 de la Ley General de Transparencia y Acceso a la Información Pública, así como la aprobación de la definición de la fecha a partir de la cual podrá presentarse la denuncia por la falta de publicación de las obligaciones de transparencia, a la que se refiere el Capítulo VII y el Título Quinto de la Ley General de Transparencia y Acceso a la Información Pública, publicados en el Diario Oficial de la Federación el 02 de noviembre de 2016. Disponible en: ***http://www.dof.gob.mx/nota_detalle.php?codigo=5459497&fecha=02/11/2016***

Solicitudes de intervención de comunicaciones <<sujeto obligado>>

Ejercicio	Periodo que se informa	Por solicitud de intervención se especificarán los siguientes datos						Denominación de la empresa concesionaria de los servicios de comunicación vía satélite o telecomunicaciones que colaboraron en el proceso de intervención	Número total de solicitudes de intervención
		Objeto de la intervención	Fundamento legal del requerimiento			Alcance temporal	Autorización judicial: Si/No		
			artículo	fracción	inciso				

- Denominación de la instancia que solicita el acceso a los registros
- Fecha en la que se realizó la solicitud con el formato día/mes/año
- Causa que motivó la solicitud
- Fundamento legal para realizar la solicitud: artículo, fracción, inciso
- Número total de solicitudes al registro de comunicaciones
- Número total de solicitudes al registro de localización geográfica

4.3.2. LINEAMIENTOS DE COLABORACIÓN EN MATERIA DE SEGURIDAD Y JUSTICIA

Solicitudes de registro de comunicaciones y de registro de localización geográfica <<sujeto obligado>>

Denominación de la instancia que solicita el acceso a los registros	Fecha en la que se realizó la solicitud día/mes/año	Causa que motivó la solicitud	Fundamento legal para realizar la solicitud artículo, fracción, inciso	Número total de solicitudes al registro de comunicaciones	Número total de solicitudes al registro de localización geográfica

Luego de un proceso de consulta pública, dentro del cual R3D participó activamente [54], el 2 de diciembre de 2015, el Instituto Federal de Telecomunicaciones (IFT) publicó en el Diario Oficial de la Federación, los Lineamientos de Colaboración en Materia de Seguridad y Justicia[55], en los que se detalla la manera en la que las empresas concesionarias de telecomunicaciones deben cumplir con las solicitudes de acceso al registro de comunicaciones y de localización geográfica en tiempo real de equipos de comunicación móvil.

El Lineamiento Décimo Octavo de este instrumento establece distintas obligaciones de transparencia relacionadas con estas medidas de vigilancia.

En primer lugar, se establece la obligación a las concesionarias y autorizadas para prestar servicios de telecomunicaciones, de entregar al IFT en los meses de enero y julio un informe semestral electrónico que debe contener el número total, por autoridad facultada, de los requerimientos de información de localización geográfica en tiempo real y de acceso al registro de comunicaciones desglosando las solicitudes recibidas, entregadas y no entregadas mensualmente. Según los Lineamientos, el IFT tiene la obligación de hacer públicos dichos informes en su sitio de Internet.

En segundo lugar, los Lineamientos también obligan al IFT a solicitar a las autoridades un informe semestral, en los meses de enero y julio de cada año, relativo al número de requerimientos de localización geográfica en tiempo real y de registro de datos realizados.

De acuerdo al artículo sexto transitorio de los Lineamientos del IFT, los informes semestrales deben de empezar a emitirse y solicitarse, respectivamente, a partir de julio de 2016.

4.4 TRANSPARENCIA Y VIGILANCIA EN LA PRÁCTICA

Al margen de los importantes avances normativos reseñados, persiste una gran dificultad para obtener información respecto a la manera en la que las facultades de vigilancia están siendo utilizadas por las autoridades, así como información respecto de cuál es el papel que juega el poder judicial en su labor de supervisión y las empresas de telecomunicaciones como colaborador de la vigilancia.

[54.] R3D presentó sus comentarios para la Consulta Pública del Anteproyecto de Lineamientos de Colaboración en Materia de Seguridad y Justicia el 27 de noviembre de 2014. Disponible en: *http://www.ift.org.mx/sites/default/files/industria/temasrelevantes/consultaspublicas/documentos/comentariosr3dconsultaift.pdf*

[55.] Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones expide los Lineamientos de Colaboración en Materia de Seguridad y Justicia publicados en el Diario Oficial de la Federación el 02 de diciembre de 2015. Disponible en: *http://dof.gob.mx/nota_detalle.php?codigo=5418339&fecha=02/12/2015*

INFORME DE CUMPLIMIENTO DE REQUERIMIENTOS DE LOCALIZACIÓN GEOGRÁFICA EN TIEMPO REAL

Fecha: ____/____/____
día / mes / año

Concesionario o Autorizado _____

Nombre del representante legal: _____
Apellido Paterno Apellido Materno Nombre(s)

i. Requerimientos recibidos de Localización geográfica en tiempo real

Meses	Autoridad 1	Autoridad 2	Autoridad 3	Autoridad ..	Autoridad n
Mes 1					
Mes 2					
Mes 3					
Mes 4					
Mes 5					
Mes 6					
Total por Autoridad	0	0	0	0	0
Número total de solicitudes recibidas de Localización Geográfica en tiempo real	0				

ii. Requerimientos entregados de Localización geográfica en tiempo real

Meses	Autoridad 1	Autoridad 2	Autoridad 3	Autoridad ..	Autoridad n
Mes 1					
Mes 2					
Mes 3					
Mes 4					
Mes 5					
Mes 6					
Total por Autoridad	0	0	0	0	0
Número total de solicitudes procesadas de Localización Geográfica en tiempo real	0				

ii. Requerimientos no entregados de Localización geográfica en tiempo real

Meses	Autoridad 1	Autoridad 2	Autoridad 3	Autoridad ..	Autoridad n
Mes 1					
Mes 2					
Mes 3					
Mes 4					
Mes 5					
Mes 6					
Total por Autoridad	0	0	0	0	0
Número total de solicitudes entregadas de Localización Geográfica en tiempo real	0				

Información Adicional

_____
Firma autógrafa del Concesionario o Autorizado o de su representante legal

INFORME DE CUMPLIMIENTO DE REQUERIMIENTOS DE DATOS CONSERVADOS

Fecha: ____/____/____
día / mes / año

Concesionario o Autorizado _____

Nombre del representante legal: _____
Apellido Paterno | Apellido Materno | Nombre(s)

i. Requerimientos recibidos de datos conservados

Meses	Autoridad 1	Autoridad 2	Autoridad 3	Autoridad ..	Autoridad n
Mes 1					
Mes 2					
Mes 3					
Mes 4					
Mes 5					
Mes 6					
Total por Autoridad	0	0	0	0	0
Número total de solicitudes recibidas de datos conservados	0				

ii. Requerimientos entregados de datos conservados

Meses	Autoridad 1	Autoridad 2	Autoridad 3	Autoridad ..	Autoridad n
Mes 1					
Mes 2					
Mes 3					
Mes 4					
Mes 5					
Mes 6					
Total por Autoridad	0	0	0	0	0
Número total de solicitudes procesadas de datos conservados	0				

iii. Requerimientos no entregados de datos conservados

Meses	Autoridad 1	Autoridad 2	Autoridad 3	Autoridad ..	Autoridad n
Mes 1					
Mes 2					
Mes 3					
Mes 4					
Mes 5					
Mes 6					
Total por Autoridad	0	0	0	0	0
Número total de solicitudes entregadas de datos conservados	0				

Información Adicional

_____
Firma autógrafa del Concesionario o Autorizado o de su representante legal

4.4.1. RETRASOS E INCUMPLIMIENTOS NORMATIVOS

A la fecha, las normas que han establecido obligaciones de transparencia respecto de las medidas de vigilancia no han significado, en la práctica, un avance sustancial en la cantidad y calidad de la información disponible sobre el volumen y alcance de las medidas de vigilancia.

La obligación de transparencia proactiva establecida en el artículo 70, fracción XLVII, de la LGTA, reconocida en las leyes federales y locales en materia de transparencia, únicamente han sido cumplida por la Fiscalía General del Estado de Querétaro, la cual ha puesto a disposición del público algunas estadísticas en su portal de Internet [56].

Como ha sido mencionado, esta obligación debía ser cumplida originalmente a partir del 4 de noviembre de 2016, sin embargo, el INAI ha prorrogado el plazo de cumplimiento hasta el 4 de mayo de 2017.

En el caso de los Lineamientos del IFT sobre colaboración en materia de seguridad y justicia, ha existido un cumplimiento parcial. Únicamente diez empresas han cumplido con la obligación de remitir el informe semestral en el mes de junio de 2016 y el IFT no ha cumplido su obligación de publicar dichos informes en su página de Internet. R3D obtuvo acceso a los mismos después de una solicitud de acceso a la información pública.

Además, el IFT no ha cumplido con la obligación asumida por sí mismo de solicitar a las autoridades un informe semestral. Ante dicha omisión, R3D interpuso una demanda de amparo en contra del IFT la cual se encuentra pendiente de resolución por el Juzgado Segundo de Distrito en Materia Administrativa, Especializado en Competencia Económica, Radiodifusión y Telecomunicaciones.

4.4.2. SOLICITUDES DE ACCESO A LA INFORMACIÓN PÚBLICA Y RECURSOS DE REVISIÓN EN MATERIA DE TRANSPARENCIA

R3D ha realizado 573 solicitudes de acceso a la información pública con la intención de obtener información estadística y acceso a versiones públicas de las solicitudes realizadas por autoridades federales y de las 32 entidades federativas, relacionadas con medidas de vigilancia, así como de las resoluciones del Poder Judicial Federal, en los casos en los que ha sido solicitada autorización judicial federal.

[56.] Portal de Internet de la Fiscalía General del Estado de Querétaro, sección de Transparencia. Disponible en: *http://fiscaliageneralqro.gob.mx/Transparencia-A66/FormatosINAI/XLVI-FormListadoEmpresasConcesionariasTelecom.pdf*

Ante la negativa de respuesta se han interpuesto 213 recursos de revisión ante los órganos garantes en materia de transparencia. Lo anterior ha dado como resultado que 10 Institutos de transparencia locales (Aguascalientes, Chiapas, Chihuahua, Ciudad de México, Coahuila, Durango, Jalisco, Oaxaca, Tabasco y Zacatecas) y el INAI hayan reconocido que la información estadística sobre medidas de vigilancia es información pública.

No obstante lo anterior, persiste gran resistencia para facilitar el acceso a información estadística, así como a versiones públicas relacionadas con las solicitudes y requerimientos formulados por autoridades al Poder Judicial de la Federación o a empresas sobre medidas de vigilancia.

Un caso paradigmático sobre la cultura de opacidad que persiste en muchas autoridades es el caso del Centro de Investigación y Seguridad Nacional (en adelante "CISEN").

Ante una solicitud de acceso a la información formulada por R3D, el CISEN se negó a informar el número de personas y dispositivos sujetos a una intervención de comunicaciones privadas en el año 2014. Ante la negativa, R3D interpuso un recurso de revisión, registrado bajo el número de expediente RDA 2149/16, el cual fue resuelto favorablemente el 25 de mayo de 2016.

No obstante, la Consejería Jurídica del Ejecutivo Federal presentó ante la Suprema Corte de Justicia de la Nación (en adelante "SCJN") un recurso de revisión en materia de seguridad nacional (el primero del año y el segundo en la historia) en contra de la resolución del INAI, argumentando que divulgar la información en solicitada por R3D pondría en riesgo la seguridad nacional.

Es importante resaltar que no se busca conocer la identidad de las personas vigiladas, ni ninguna circunstancia específica sobre una amenaza a la seguridad nacional, sino que lo único que se pretende conocer es el número de personas y dispositivos relacionados con intervenciones de comunicaciones privadas en 2014, algo que de ninguna manera puede considerarse que pueda representar un riesgo real e identificable a la seguridad nacional.

Con 10 votos a favor y uno en contra, el 5 de diciembre de 2016, la Suprema Corte de Justicia de la Nación desechó el recurso del Consejero Jurídico de la Federación para impedir la revelación de datos estadísticos sobre vigilancia (Recurso de Revisión en Materia de Seguridad Nacional 1/2016).

Otro obstáculo que persiste para la transparencia sobre la vigilancia es la falta de acceso a versiones pùblicas de las solicitudes de autorización judicial para llevar a cabo medidas de vigilancia, los requerimientos a empresas para colaborar con medidas de vigilancia y las resoluciones de autoridades judiciales autorizando o negando las solicitudes de autoridades.

[redacted]

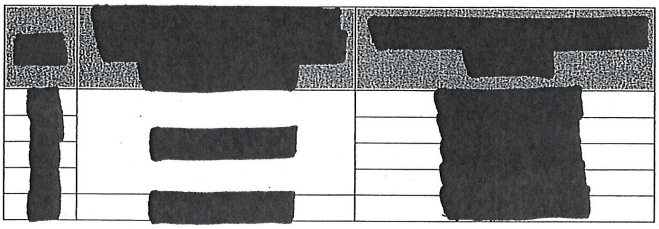
SEGOB
SECRETARÍA DE GOBERNACIÓN

ESTADOS UNIDOS MEXICANOS

CNS
COMISIÓN NACIONAL DE SEGURIDAD

POLICÍA FEDERAL

[redacted]



[redacted]

El acceso a versiones públicas de dichos documentos es sumamente importante, en tanto se han detectado inconsistencias en la información estadística publicada por las autoridades y, en diversas ocasiones, las autoridades han negado el acceso a información estadística relevante bajo el pretexto de no contar con la información estadística desagregada con el nivel de detalle solicitado. En este sentido, acceder a las versiones públicas de dichos documentos es esencial para constatar y medir con precisión y certeza documental la cantidad de solicitudes, requerimientos y autorizaciones relacionadas con medidas de vigilancia, el número de personas o dispositivos objeto de vigilancia, las categorías de datos vigiladas, la duración de las medidas, los motivos generales de las solicitudes y requerimientos, los fundamentos legales empleados, los criterios generales adoptados por la autoridad judicial para resolver las solicitudes de autorización de medidas de vigilancia, entre otros datos.

Es importante resaltar que la revelación de estos datos en ningún caso pone en riesgo la integridad de una investigación criminal u obstaculiza la atención de una amenaza a la seguridad nacional puesto que no revela datos que identifiquen a las personas o dispositivos vigilados, ni las circunstancias específicas de las situaciones bajo investigación, dado que estos pueden ser testados de las versiones públicas entregadas.

R3D ha logrado que algunos órganos garantes reconozcan la publicidad de las versiones públicas, sin embargo, otros como el INAI han adoptado interpretaciones en las que se lleva a cabo una reserva absoluta de información, por ejemplo, en materia de seguridad nacional, en donde el INAI ha considerado que la información relacionada con esta materia es reservada totalmente por virtud del artículo 51 de la Ley de Seguridad Nacional[57].

Adicionalmente, en algunos casos las versiones públicas otorgadas por las autor idades realizan un testado excesivo o absoluto de los documentos de manera que no se puede conocer información de interés público sobre las actividades de vigilancia.

[57.] INAI. Recurso de Revisión RRA 2100/16 resuelto por el Pleno del INAI en sesión celebrada el día 1 de noviembre de 2016. Página 64.

4.4.3. EL DERECHO A CONOCER LOS METADATOS DE COMUNICACIONES CONSERVADOS POR LAS EMPRESAS DE TELECOMUNICACIONES

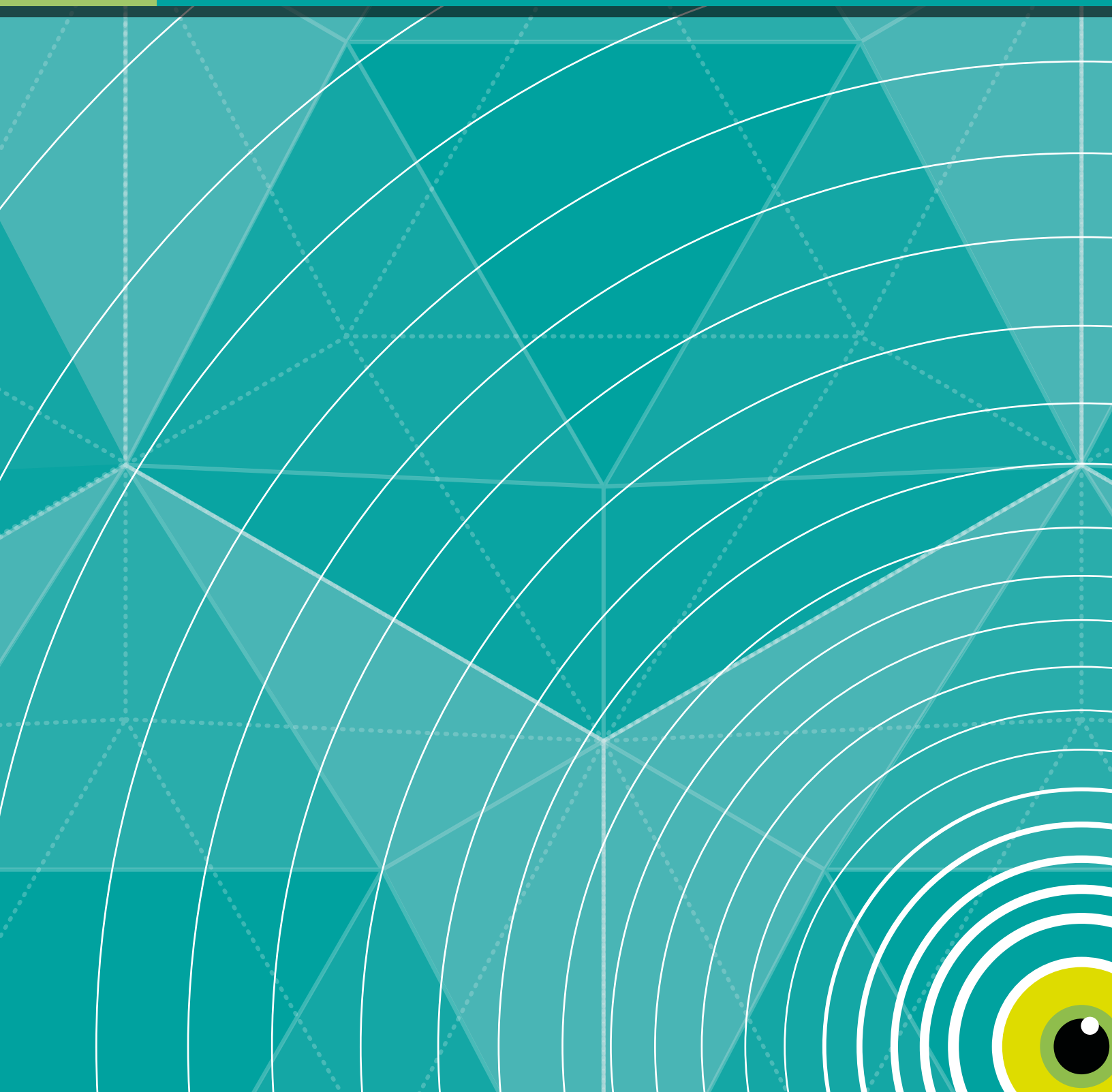
Otra de las vías que R3D ha utilizado para transparentar la manera en la que se interfiere con la privacidad de las personas es utilizando los derechos de protección de datos personales, en particular el derecho de acceso.

En concreto, integrantes de R3D han solicitado a las tres empresas de telefonía móvil más importantes en el país (AT&T, Telcel y Telefónica Movistar) acceso a sus datos conservados por las empresas de telecomunicaciones, incluyendo los metadatos de comunicaciones retenidos por virtud del artículo 190, fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión, incluyendo el historial de comunicaciones, la fecha, hora y duración de las mismas, así como la localización geográfica de los usuarios de telecomunicaciones durante la comunicación.

Las tres empresas negaron el acceso a los datos personales, aduciendo una supuesta imposibilidad legal, e incluso, que entregar a un usuario sus datos de comunicaciones podría afectar la seguridad nacional. Ante la negativa, R3D inició procedimientos de protección de derechos ante el INAI, el cual ya ha resuelto los procedimientos interpuestos respecto de AT&T (PPD.0083/16) y Telcel (PPD.0104/16), restando por resolverse el procedimiento relativo a Telefónica Movistar.

En la resolución favorable de dichos procedimientos, el INAI ha reconocido que los datos de comunicaciones que las empresas conservan, por virtud del artículo 190, fracción II, son datos personales y las empresas deben entregarlos cuando les sean solicitados por los usuarios. No obstante lo anterior, a la fecha las resoluciones no han sido cumplidas en su totalidad.

5 LA VIGILANCIA EN NÚMEROS



Por más de un año, R3D ha llevado a cabo una investigación sobre cómo es la vigilancia estatal en la práctica, un aspecto que ha sido muy poco documentado. Nuestro método se ha centrado en el análisis de cerca de 600 solicitudes de acceso a la información pública realizadas a autoridades federales y de las entidades federativas con la intención de conocer estadísticas sobre el uso de las diversas medidas de vigilancia en los años 2013, 2014 y 2015. También se solicitó información al Poder Judicial Federal sobre la solicitudes de autorización judicial para llevar a cabo dichas medidas y se obtuvo acceso a los reportes enviados por concesionarias de telecomunicaciones al Instituto Federal de Telecomunicaciones (IFT) relativos al primer semestre de 2016.

En particular, se preguntó a autoridades federales [58] y de las entidades federativas [59] cuestiones como el número de ocasiones en las que solicitaron autorización judicial federal para llevar a cabo una medida de vigilancia, el número de ocasiones en las que lo hicieron sin autorización judicial, datos sobre el número de personas o dispositivos afectados por las medidas de vigilancia y datos sobre el número de averiguaciones previas en las que se utilizaron medidas de vigilancia y su estado procesal.

A pesar de los obstáculos que algunas autoridades interpusieron para acceder a la información solicitada, lo cual implicó interponer más de 200 recursos de revisión ante órganos garantes de la transparencia en todo el país y en algunos casos aún no ha sido posible acceder a la información [60], a continuación se presentan los hallazgos de la investigación hasta noviembre de 2016.

[58.] Ver Nota Metodológica.

[59.] Ver Nota Metodológica.

[60.] Por ejemplo, La Fiscalía General del Estado de Aguascalientes, la Procuraduría General de Justicia de la Ciudad de México, la Procuraduría General de Justicia del Estado de Guanajuato y la Comisión Federal de Competencia Económica no han entregado información alguna. Otras autoridades como la Procuraduría General de la República (PGR), el Centro de Investigación y Seguridad Nacional (CISEN), Fiscalía General del Estado de Quintana Roo, la Procuraduría General de Justicia del Estado de Chiapas, entre otras, no han entregado información de manera parcial.

TABLA DE ABREVIATURAS	
Intervención de comunicaciones privadas	**ICP**
Acceso a datos conservados	**ADC**
Solicitud de acceso a la información pública	**SAI**
Centro de Investigación y Seguridad Nacional	**CISEN**
Comisión Nacional de Seguridad - Policía Federal	**POLICÍA FEDERAL**
Procuraduría General de la República	**PGR**
Consejo de la Judicatura Federal	**CJF**
Secretaría de Comunicaciones y Transportes	**SCT**
Secretaría de Hacienda y Crédito Público	**SHCP**
Instituto Electoral del Distrito Federal	**IEDF**
Fiscalía General del Estado de Aguascalientes	**FGE AGUASCALIENTES**
Procuraduría General de Justicia del Estado de Baja California	**FGE BC**
Procuraduría General de Justicia del Estado de Baja California Sur	**PGJE BCS**
Fiscalía General del Estado de Campeche	**FGE CAMPECHE**
Procuraduría General de Justicia del Estado de Chiapas	**PGJE CHIAPAS**
Fiscalía General del Estado de Chihuahua	**FGE CHIHUAHUA**
Procuraduría General de Justicia del Estado de Coahuila	**PGJE COAHUILA**
Procuraduría General de Justicia del Estado de Colima	**PGJE COLIMA**
Procuraduría General de Justicia de la Ciudad de México	**PGJ CDMX**
Fiscalía General del Estado de Durango	**FGE DURANGO**
Procuraduría General de Justicia del Estado de México	**PGJ EDOMEX**
Procuraduría General de Justicia del Estado de Guanajuato	**PGJE GUANAJUATO**
Fiscalía General del Estado de Guerrero	**FGE GUERRERO**
Procuraduría General de Justicia del Estado de Hidalgo	**PGJE HIDALGO**
Fiscalía General del Estado de Jalisco	**FGE JALISCO**
Procuraduría General de Justicia del Estado de Michoacán	**PGJE MICHOACÁN**
Fiscalía General del Estado de Morelos	**FGE MORELOS**

TABLA DE ABREVIATURAS	
Fiscalía General del Estado de Nayarit	**FGE NAYARIT**
Procuraduría General de Justicia del Estado de Nuevo León	**PGJE NUEVO LEÓN**
Fiscalía General del Estado de Oaxaca	**FGE OAXACA**
Fiscalía General del Estado de Puebla	**FGE PUEBLA**
Fiscalía General del Estado de Querétaro	**FGE QUERETARO**
Fiscalía General del Estado de Quintana Roo	**FGE QUINTANA ROO**
Procuraduría General de Justicia del Estado de San Luis Potosí	**PGJE SLP**
Procuraduría General de Justicia del Estado de Sinaloa	**PGJE SINALOA**
Procuraduría General de Justicia del Estado de Sonora	**PGJE SONORA**
Fiscalía General del Estado de Tabasco	**FGE TABASCO**
Procuraduría General de Justicia del Estado de Tamaulipas	**PGJE TAMAULIPAS**
Procuraduría General de Justicia del Estado de Tlaxcala	**PGJE TLAXCALA**
Fiscalía General del Estado de Veracruz	**FGE VERACRUZ**
Fiscalía General del Estado de Yucatán	**FGE YUCATÁN**
Procuraduría General de Justicia del Estado de Zacatecas	**PGJE ZACATECAS**
Policía Cibernética de Querétaro	**PC QUERÉTARO**
Gobierno del Estado de Colima	**G. COLIMA**
Gobierno del Estado de México	**G. EDOMEX**
Sistema Estatal de Seguridad Pública de Baja California	**SESPBC**
Tribunal Superior de Justicia de la Ciudad de México	**TSJ CDMX**

5.1 INTERVENCIÓN DE COMUNICACIONES PRIVADAS

Entre 2013 y 2015, se ha documentado la realización de 3182 solicitudes de autorización judicial para llevar a cabo la **intervención de comunicaciones privadas (ICP)**. El CISEN es la autoridad que más veces ha hecho este tipo de intervenciones, seguido de la PGR y la Policía Federal.

Según datos de las propias autoridades, en casi todos los casos el poder judicial autoriza sus solicitudes de ICP. En 2013, de 872 solicitudes, únicamente 54 fueron negadas por un juez. En 2014, de 1165 solicitudes, únicamente 52 fueron negadas. En 2015, de 1144 solicitudes, fueron negadas 62. *[Ver figuras 1, 2 y 3]*

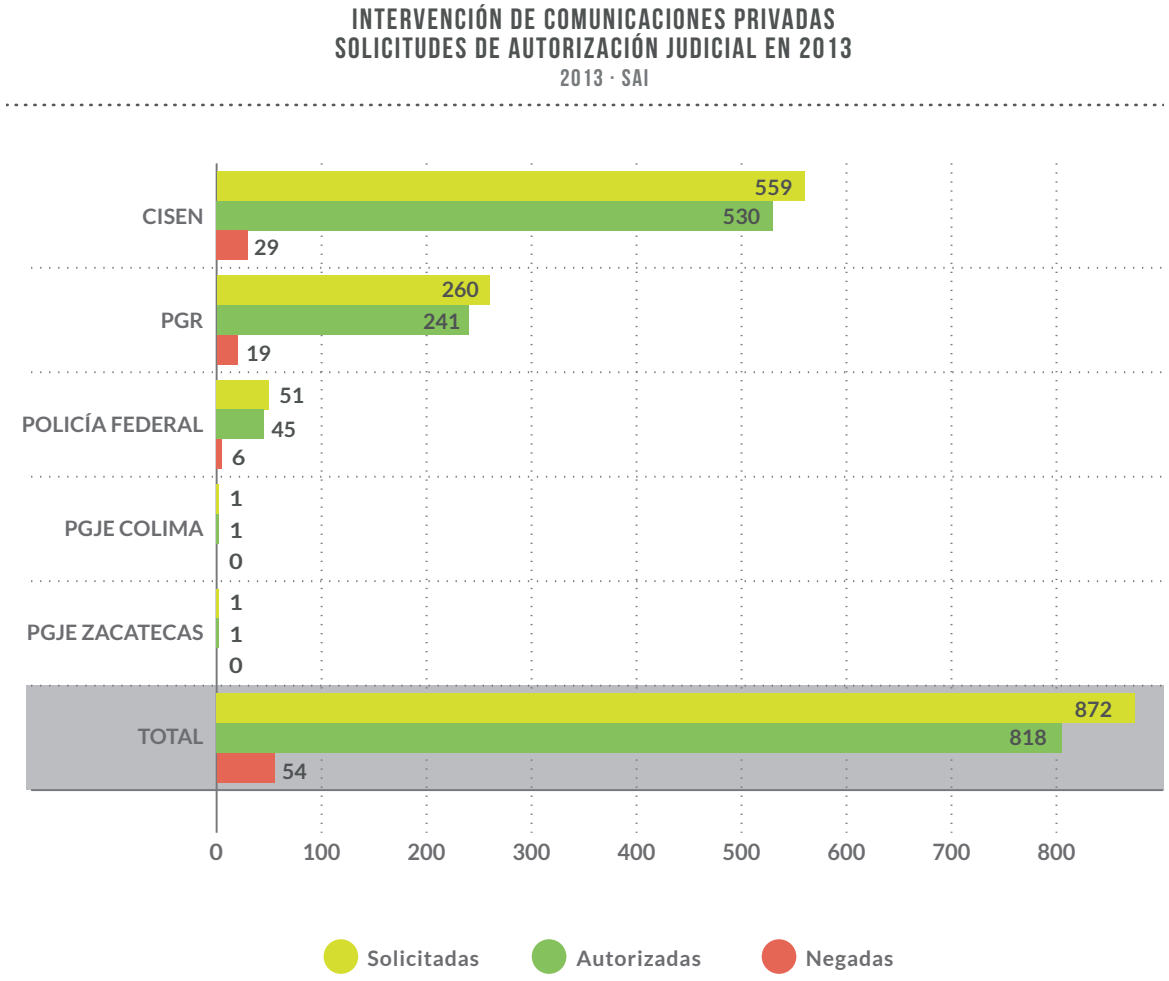
Puede observarse que en 2014 creció de manera importante el número de solicitudes de ICP respecto de 2013, sin embargo en 2015 la cifra parece haberse estabilizado. En suma, durante todo el periodo de 2013 a 2015, únicamente el 5.28% de las solicitudes documentadas fue rechazada por la autoridad judicial. *[Ver figura 4]*

No obstante lo anterior, al observar los datos aportados por el Consejo de la Judicatura Federal (CJF), aparecen graves inconsistencias. En primer lugar, el CJF únicamente reporta haber recibido solicitudes de autorización para la intervención de comunicaciones privadas únicamente de 4 autoridades: CISEN, PGR, la Policía Federal y la Procuraduría General de Justicia del Estado de Nuevo León en una ocasión. Esta información, contrasta con la presentada por su contraparte.

Y es que el CJF no hace mención de ninguna solicitud de autorización judicial realizada por la PGJE Colima, PGJE Zacatecas, FGE Tabasco, FGE Guerrero, FGE Jalisco, FGE Puebla, FGE Querétaro o FGE Quintana Roo, a pesar de que en solicitudes realizadas a dichas autoridades, éstas afirmaron haber solicitado autorización judicial en varias ocasiones. En cambio, la PGJE de Nuevo León (citada por el CJF como solicitante) no informó de ninguna solicitud de intervención de comunicaciones en su respuesta a las solicitudes de acceso a la información (SAI) formuladas por R3D.

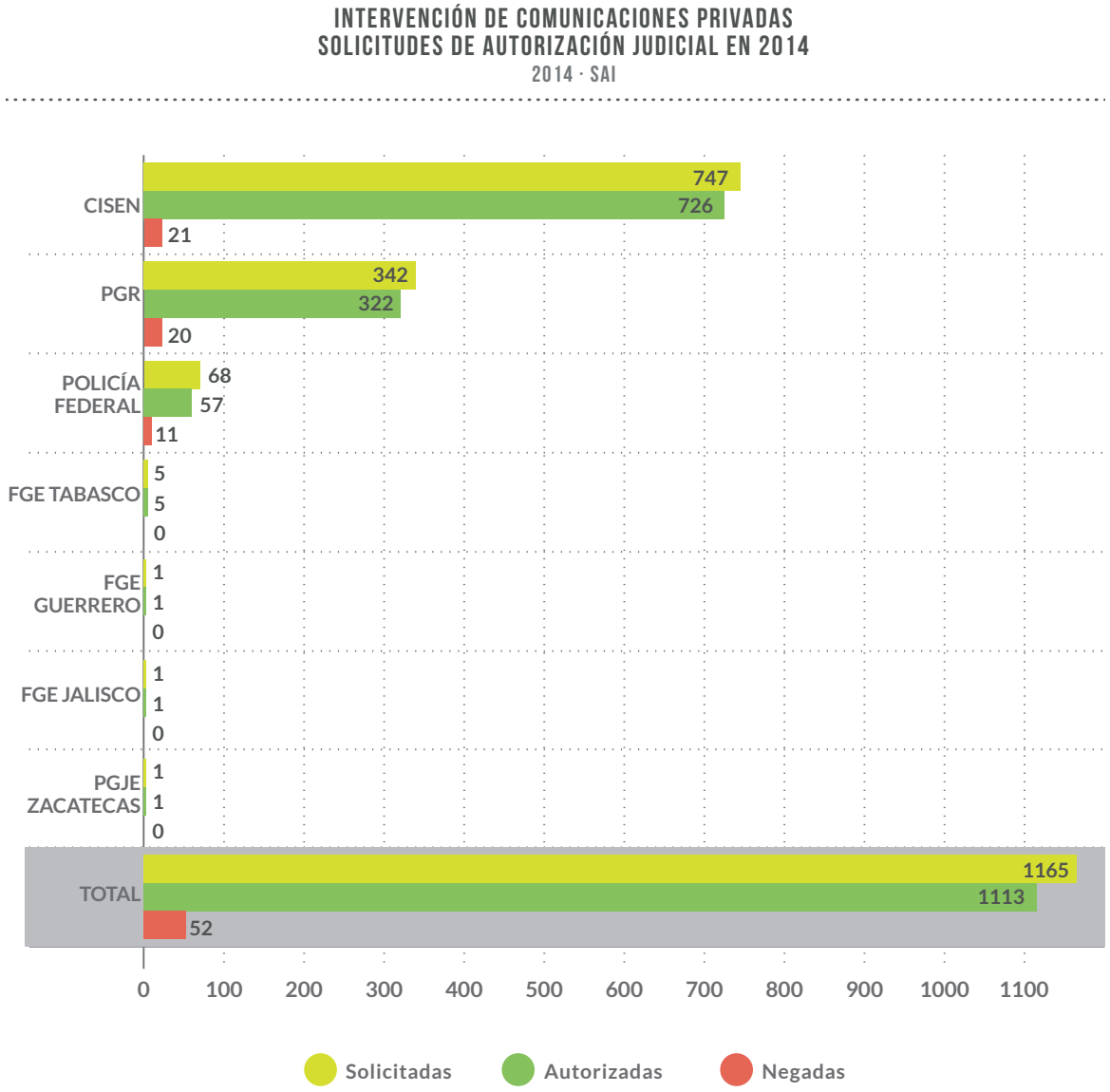
Asimismo, existen considerables discrepancias entre el número de solicitudes de autorización para las ICP reportadas por el CISEN, PGR y Policía Federal y las que el CJF reporta haber recibido de dichas autoridades. *[Ver figura 5]*

Figura 1



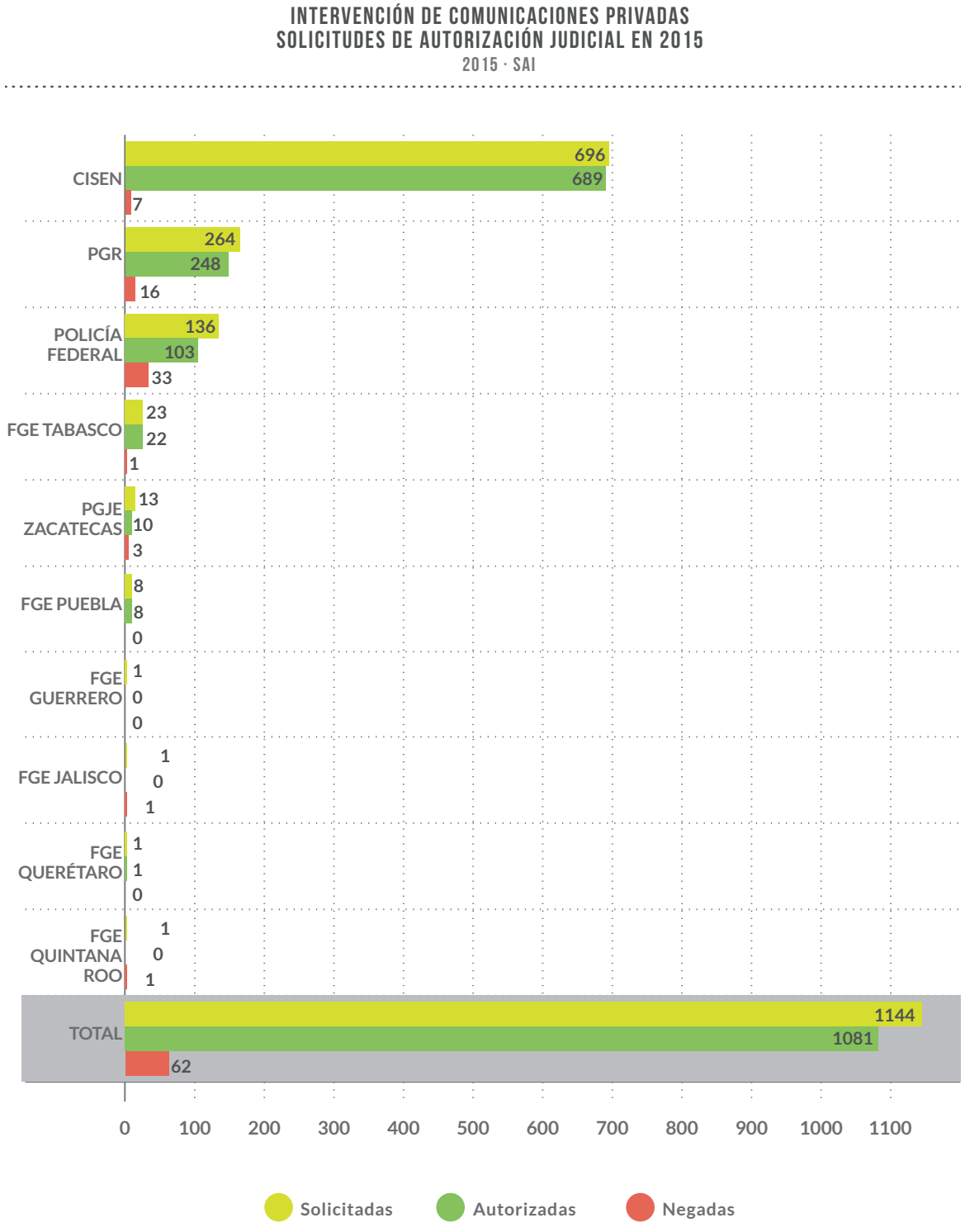
[Figura 1] Datos obtenidos a partir de respuestas a solicitudes de acceso a la información pública realizadas a autoridades federales y de las 32 entidades federativas. La Fiscalía General del Estado de Aguascalientes, la Procuraduría General de Justicia de la Ciudad de México y la Procuraduría General de Justicia del Estado de Guanajuato no entregaron información.

Figura 2



[Figura 2] Datos obtenidos a partir de respuestas a solicitudes de acceso a la información pública realizadas a autoridades federales y de las 32 entidades federativas. La Fiscalía General del Estado de Aguascalientes, la Procuraduría General de Justicia de la Ciudad de México y la Procuraduría General de Justicia del Estado de Guanajuato no entregaron información.

Figura 3



[Figura 3] Datos obtenidos a partir de respuestas a solicitudes de acceso a la información pública realizadas a autoridades federales y de las 32 entidades federativas. La Fiscalía General del Estado de Aguascalientes, la Procuraduría General de Justicia de la Ciudad de México y la Procuraduría General de Justicia del Estado de Guanajuato no entregaron información.

Figura 4

INTERVENCIÓN DE COMUNICACIONES PRIVADAS
SOLICITUDES DE AUTORIZACIÓN JUDICIAL POR AÑO
2013-2015 · SAI

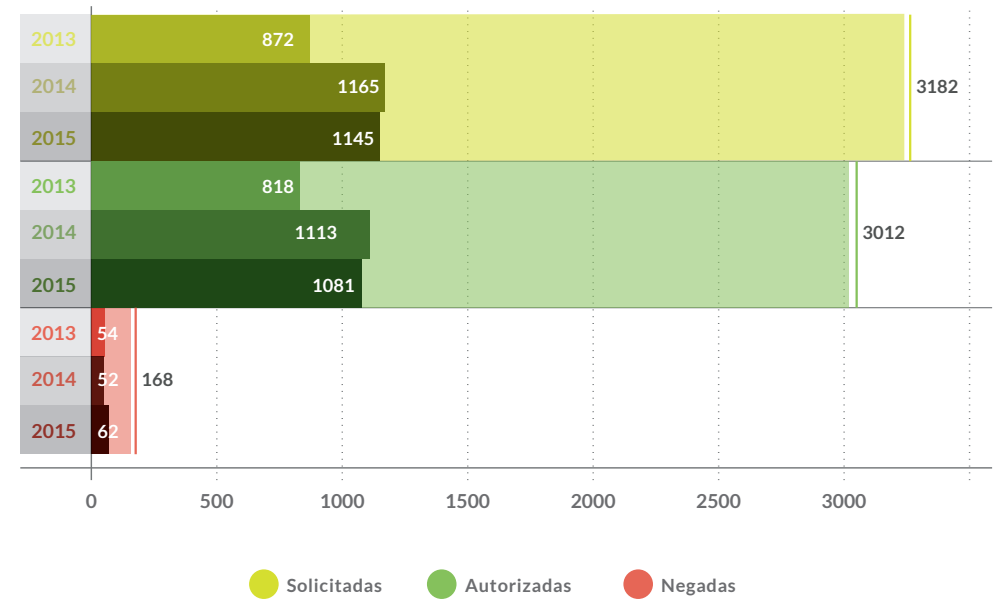
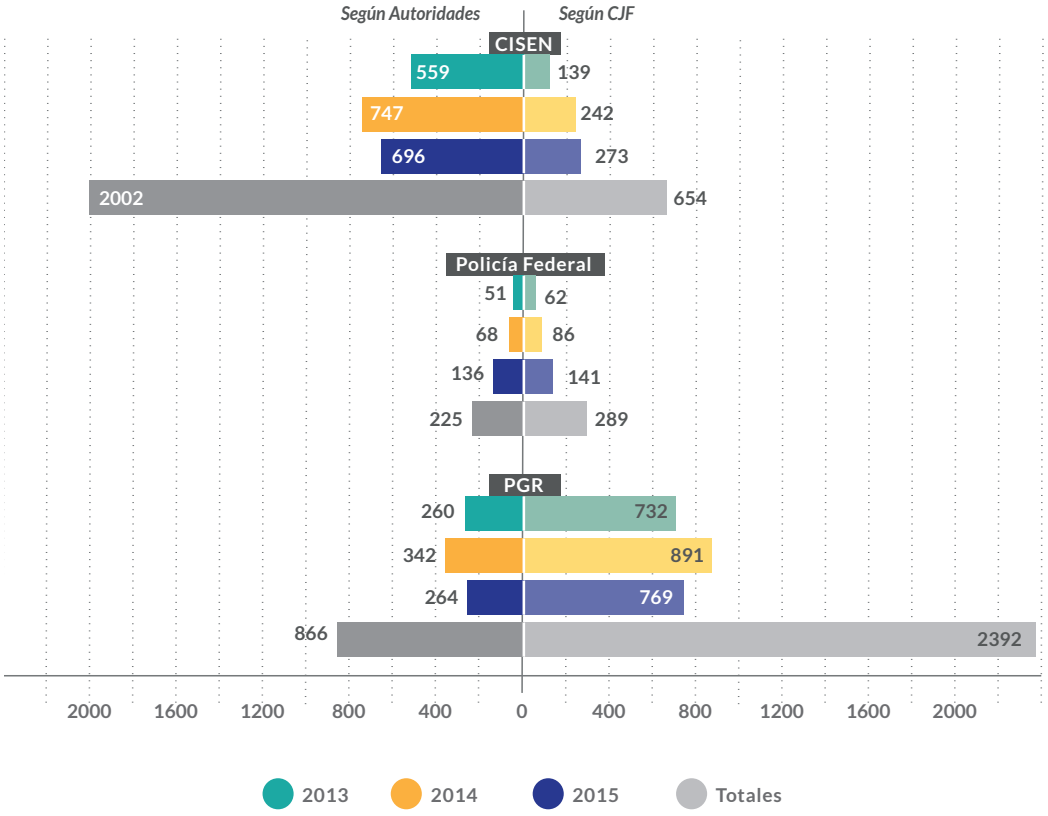


Figura 5

INTERVENCIÓN DE COMUNICACIONES PRIVADAS
SOLICITUDES DE AUTORIZACIÓN JUDICIAL SEGÚN AUTORIDADES VS DATOS DEL CJF
2013-2015 · SAI - CJF

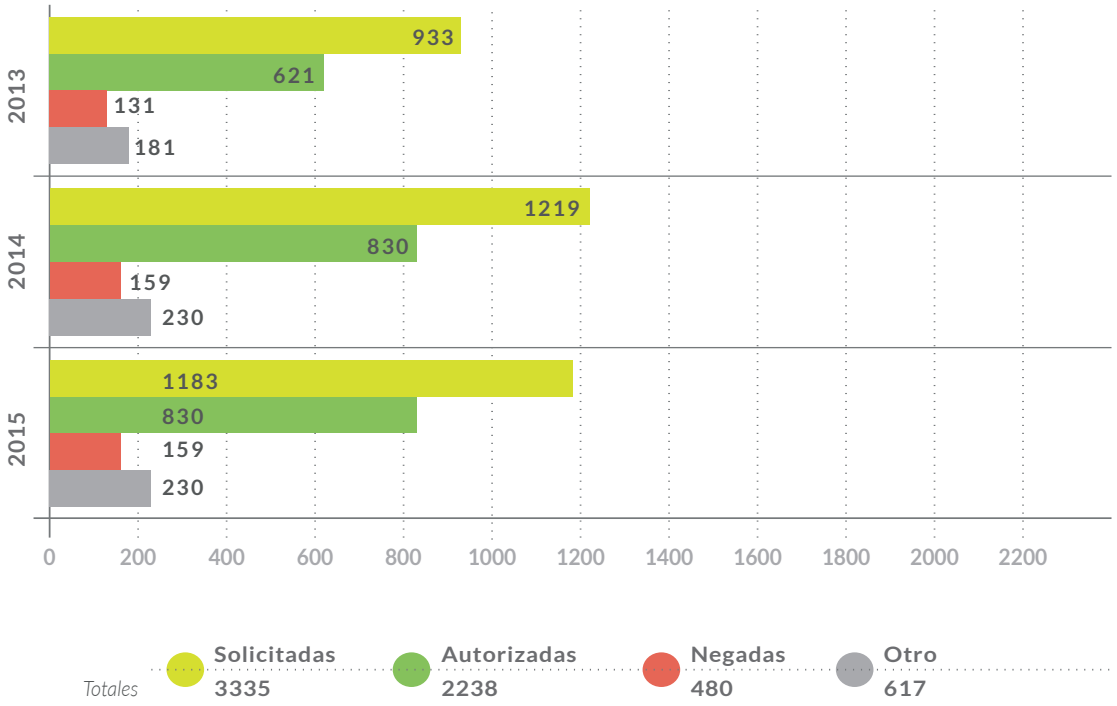


De acuerdo a los datos del CJF, entre 2013 y 2015, recibió 3335 solicitudes de ICP de parte de las tres autoridades federales, de las cuales el 67.1% fueron autorizadas total o parcialmente, el 14.39% fueron negadas y en 18.5% de las veces se adoptó una resolución distinta no especificada.

Figura 6

SOLICITUDES DE INTERVENCIÓN DE COMUNICACIONES PRIVADAS POR AÑO

2013-2015 · CJF



Es importante señalar que el número de solicitudes de autorización de ICP no es equivalente al número de personas vigiladas ya que en una sola solicitud puede buscarse la autorización para vigilar a múltiples personas o dispositivos.

[Figura 4] Datos obtenidos a partir de respuestas a solicitudes de acceso a la información pública realizadas a autoridades federales y de las 32 entidades federativas. La Fiscalía General del Estado de Aguascalientes, la Procuraduría General de Justicia de la Ciudad de México y la Procuraduría General de Justicia del Estado de Guanajuato no entregaron información.

[Figura 5] Datos obtenidos a partir de respuestas a solicitudes de acceso a la información pública realizadas a autoridades federales y al Consejo de la Judicatura Federal (CJF). Según datos del CJF, únicamente el CISEN, la Policía Federal, la PGR y la Procuraduría General de Justicia del Estado de Nuevo León (en una ocasión), solicitaron la autorización para llevar a cabo la intervención de comunicaciones privadas entre 2013 y 2015.

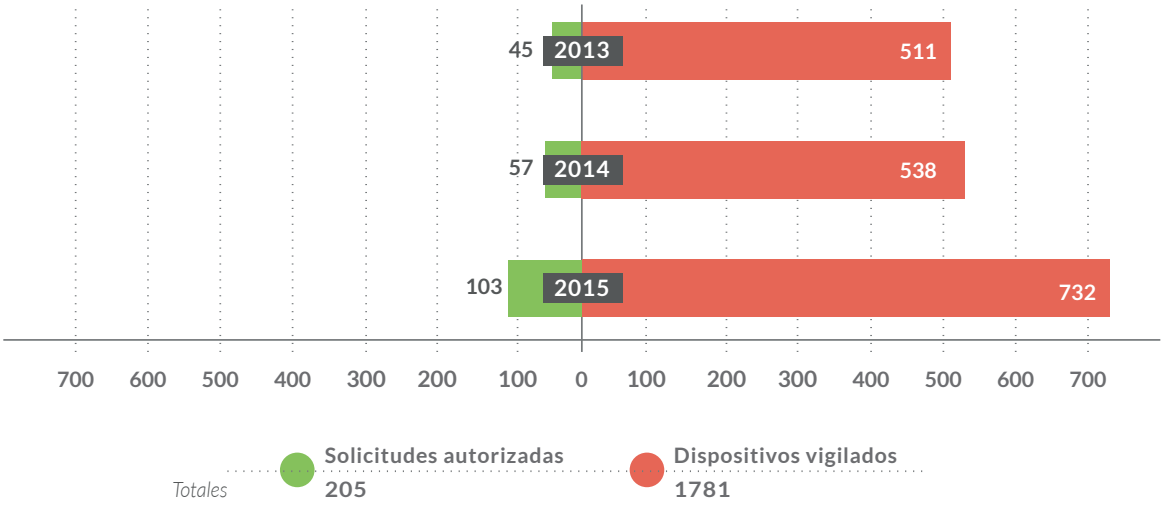
[Figura 6] Datos obtenidos a partir de respuestas a solicitudes de acceso a la información pública realizadas al Consejo de la Judicatura Federal (CJF). Según datos del CJF, únicamente el CISEN, la Policía Federal, la PGR y la PGJE Nuevo León (en una ocasión), solicitaron la autorización para llevar a cabo la intervención de comunicaciones privadas entre 2013 y 2015.

Por ejemplo, entre 2013 y 2015, fueron autorizadas 205 solicitudes realizadas por la Policía Federal, sin embargo en ese periodo vigiló 1781 dispositivos producto de esas autorizaciones. En el mismo sentido, la PGR recibió autorización respecto de 811 solicitudes y vigiló a 3672 dispositivos.

Figura 7

NÚMERO DE INTERVENCIONES DE COMUNICACIONES PRIVADAS VS DISPOSITIVOS VIGILADOS (POLICÍA FEDERAL)

2013-2015 · SAI

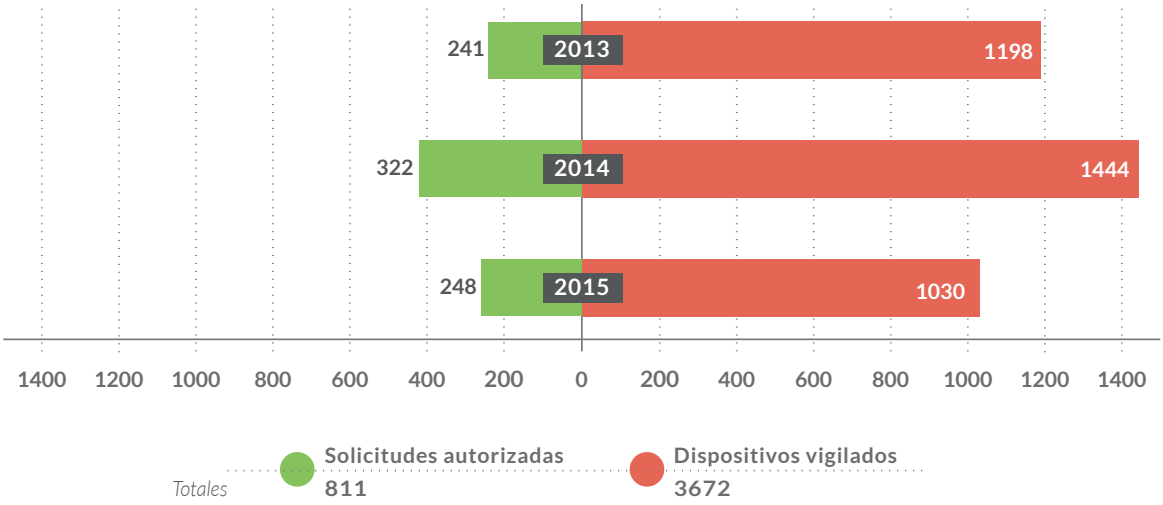


Totales

Figura 8

NÚMERO DE INTERVENCIONES DE COMUNICACIONES PRIVADAS VS DISPOSITIVOS VIGILADOS (PGR)

2013-2015 · SAI



Totales

[Figura 7] Datos obtenidos a partir de respuestas a solicitudes de acceso a la información pública realizadas a la Policía Federal.
[Figura 8] Datos obtenidos a partir de respuestas a solicitudes de acceso a la información pública realizadas a la PGR.

5.2 ACCESO A DATOS CONSERVADOS

Desde el año 2009, las empresas de telecomunicaciones se encuentran obligadas a conservar una gran cantidad de datos (conocidos como "metadatos de comunicaciones") de todos sus usuarios. Sin embargo, la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR) de 2014 expandió esta obligación al aumentar el plazo de conservación de los datos a dos años y, debido a la ambigüedad de la redacción, provocó interpretaciones diversas en torno a qué autoridades se encontraban facultadas para el acceso a los datos conservados (ADC) y si era necesaria autorización judicial.

Si bien, debido a recientes modificaciones legales e interpretaciones de parte de la SCJN ya se encuentra claras algunas de estas cuestiones [61], los datos obtenidos a partir de SAI revelan graves inconsistencias en el ejercicio de esta facultad de vigilancia entre los años 2013 y la primera mitad de 2016.

Según datos aportados por autoridades federales y de las entidades federativas, en 2013 se realizaron al menos 8867 solicitudes de ADC. En 2014 se realizaron 18111 solicitudes y en 2015 fueron 14129 los requerimientos a empresas de telecomunicaciones. El aumento considerable de solicitudes a partir del año 2014 podría ser explicado por la entrada en vigor de la LFTR a mediados de ese año. *[Ver figuras 9, 10 y 11]*

De todas las solicitudes de ADC a empresas de telecomunicaciones, únicamente el 1.09% contó con autorización judicial federal. Lo anterior implica que la gran mayoría de las solicitudes no fueron realizadas conforme a lo que establece la Constitución *[Ver figura 12]*.

[61] Por ejemplo, el amparo promovido por R3D en esta materia fue resuelto por la SCJN en mayo de 2016.

[Figura 9] Datos obtenidos a partir de respuestas a solicitudes de acceso a la información pública realizadas a autoridades federales y de las 32 entidades federativas. La Fiscalía General del Estado de Aguascalientes, la Fiscalía General del Estado de Chihuahua, la Procuraduría General de Justicia de la Ciudad de México y la Procuraduría General de Justicia del Estado de Guanajuato no entregaron información.

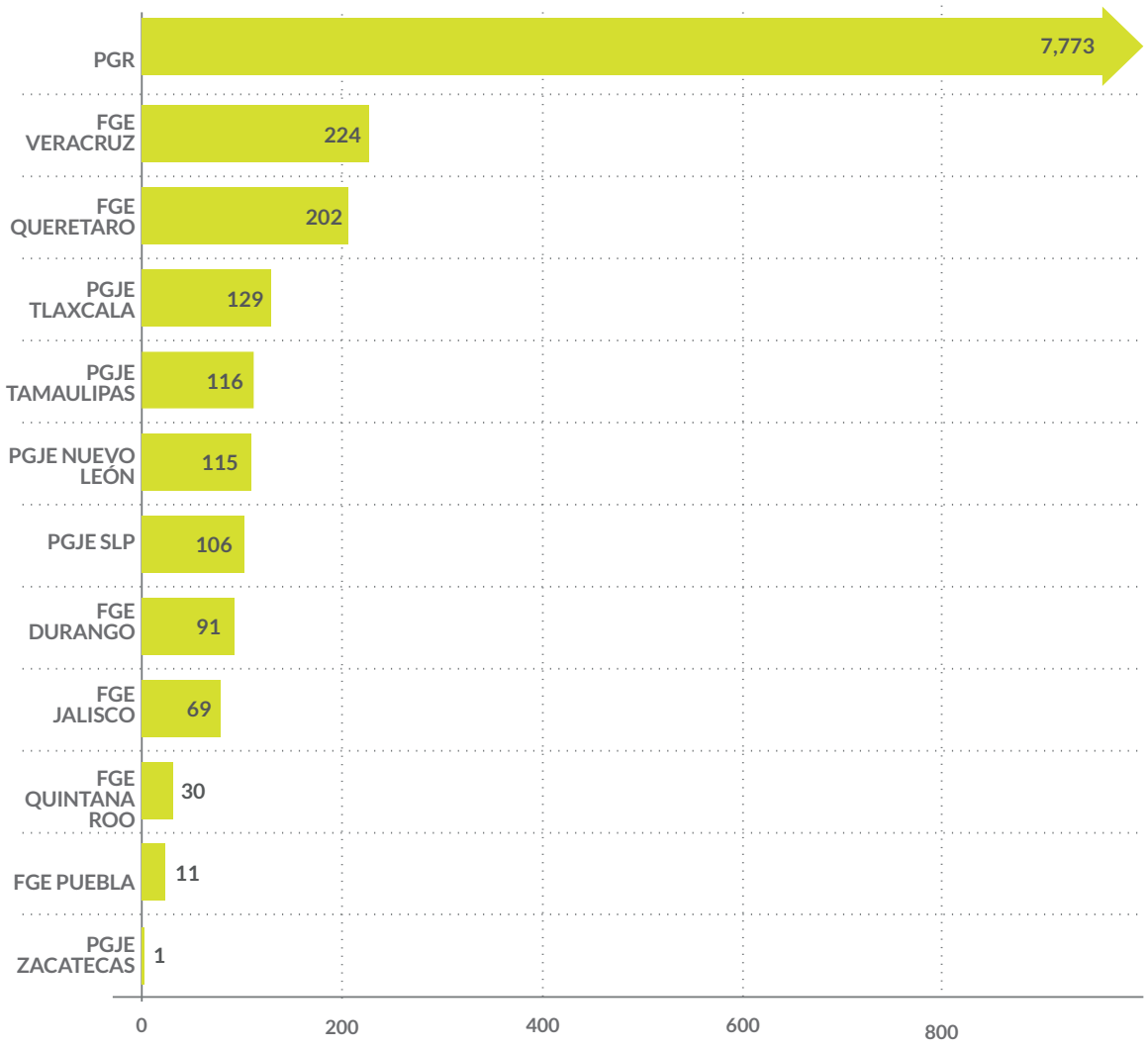
[Figura 10] Datos obtenidos a partir de respuestas a solicitudes de acceso a la información pública realizadas a autoridades federales y de las 32 entidades federativas. La Fiscalía General del Estado de Aguascalientes, la Procuraduría General de Justicia de la Ciudad de México y la Procuraduría General de Justicia del Estado de Guanajuato no entregaron información.

[Figura 11] Datos obtenidos a partir de respuestas a solicitudes de acceso a la información pública realizadas a autoridades federales y de las 32 entidades federativas. La Fiscalía General del Estado de Aguascalientes, la Procuraduría General de Justicia de la Ciudad de México, la Procuraduría General de Justicia del Estado de Guanajuato y la Comisión Federal de Competencia Económica no entregaron información.

Figura 9

SOLICITUDES DE ACCESO A DATOS CONSERVADOS POR EMPRESAS DE TELECOMUNICACIONES - 2013

2013 · SAI



Totales

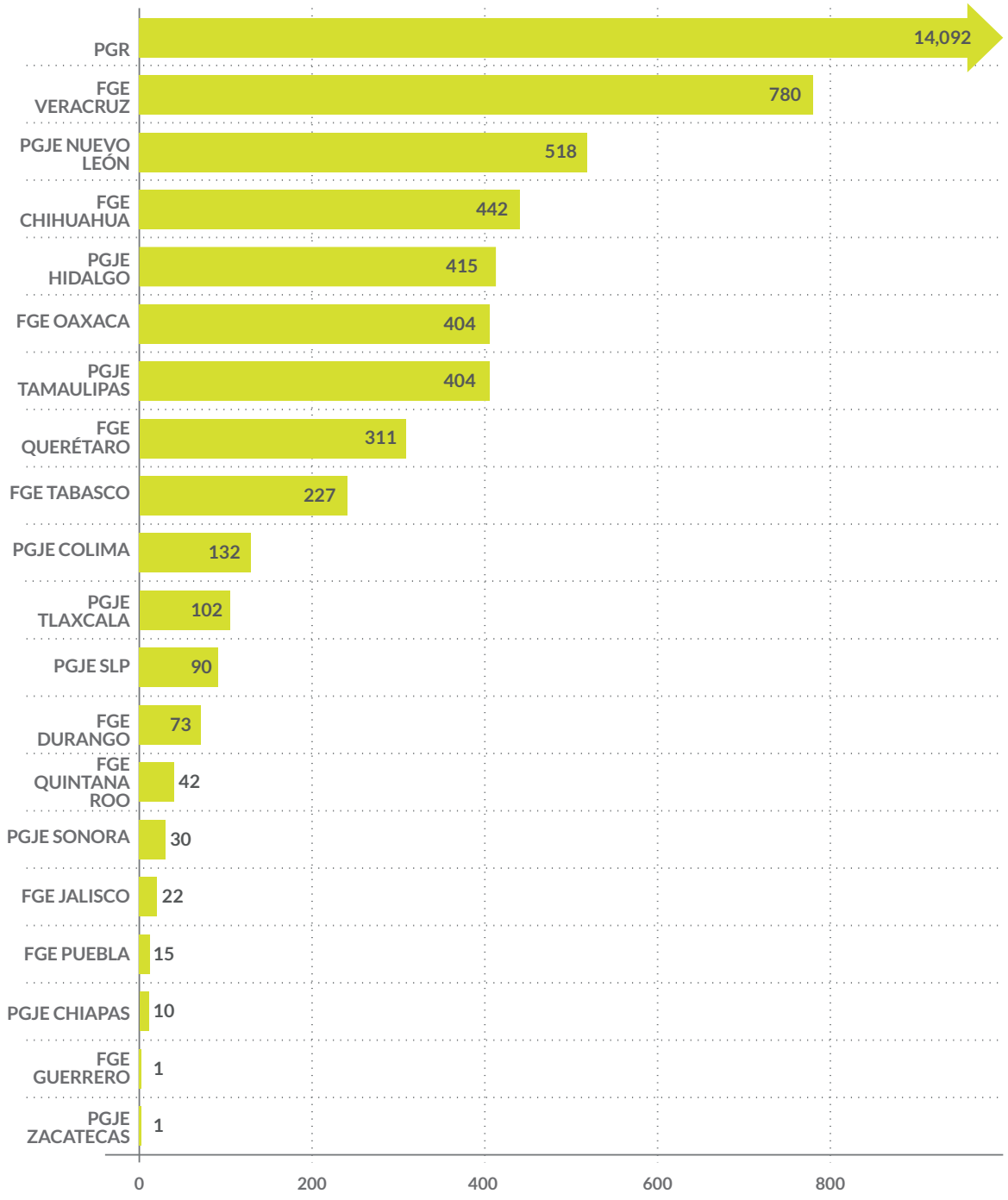
Solicitudes

8,867

Figura 10

SOLICITUDES DE ACCESO A DATOS CONSERVADOS POR EMPRESAS DE TELECOMUNICACIONES - 2014

2014 · SAI

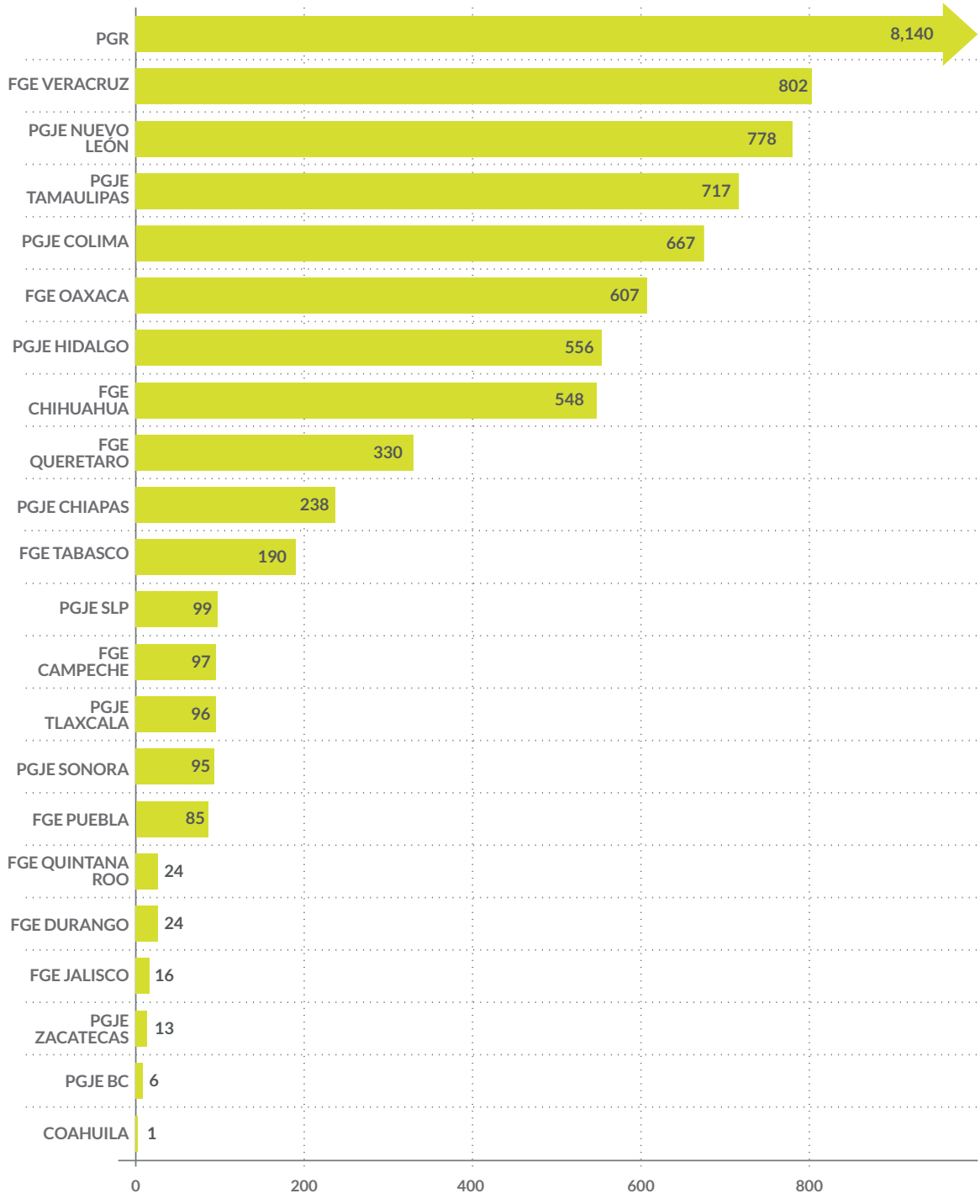


Totales Solicitudes **18,111**

Figura 11

SOLICITUDES DE ACCESO A DATOS CONSERVADOS POR EMPRESAS DE TELECOMUNICACIONES - 2015

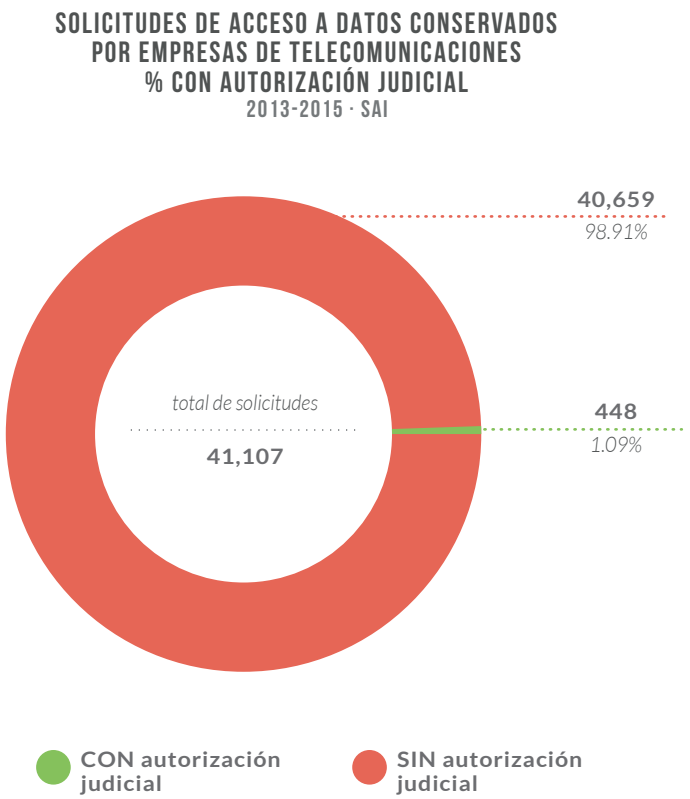
2015 · SAI



Solicitudes

Totales **14,129**

Figura 12



Como se advirtió anteriormente para el caso de las ICP, es importante señalar que el número de solicitudes de ADC no equivale al número de afectados, cuentas o dispositivos respecto de los cuáles se solicita información, pues en una sola solicitud se pueden requerir el ADC de varios usuarios.

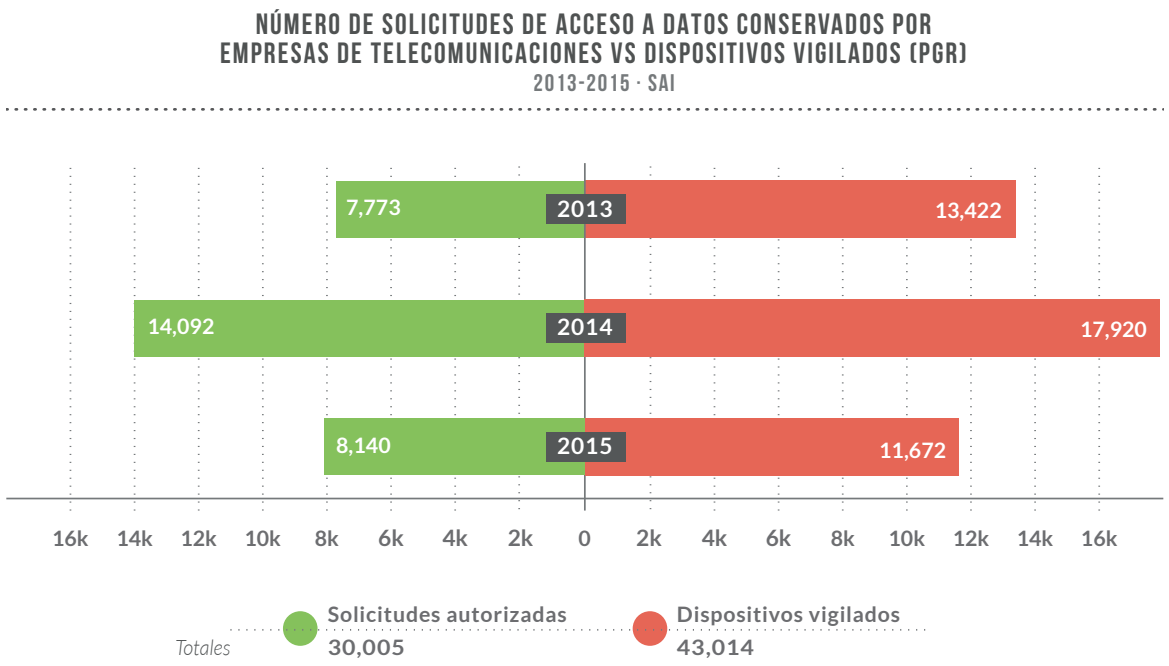
Por ejemplo, la PGR informa haber realizado 30005 solicitudes de ADC a empresas de telecomunicaciones, sin embargo accedió a los datos relacionados con 43014 dispositivos *[Ver figura 13]*.

Los datos obtenidos revelan que el número de autoridades que han realizado solicitudes de ADC también ha aumentado a partir de 2014, aunque el número real podría ser mayor.

Según datos que se desprenden de los reportes semestrales enviados por las empresas de telecomunicaciones al Instituto Federal de Telecomunicaciones (IFT), en la primera

[Figura 12] Datos obtenidos a partir de respuestas a solicitudes de acceso a la información pública realizadas a autoridades federales y de las 32 entidades federativas. La Fiscalía General del Estado de Aguascalientes, la Procuraduría General de Justicia de la Ciudad de México y la Procuraduría General de Justicia del Estado de Guanajuato no entregaron información. La Fiscalía General del Estado de Chihuahua no entregó información respecto del año 2013 y la Comisión Federal de Competencia Económica no entregó información respecto de 2015.

Figura 13



mitad de 2016, más de 46 autoridades solicitaron ADC. Es probable que el número real de autoridades que realizaron solicitudes entre 2013 y 2015 sea mayor al revelado por las propias autoridades solicitantes. *[Ver figura 14]*

Del número total de solicitudes de ADC recibidas por las 10 empresas de telecomunicaciones que cumplieron con la obligación de remitir al IFT su informe semestral respecto del primer semestre de 2016, el 71.9% fueron recibidas por Telcel, el 15.4% por AT&T y el 11.5% por Movistar; cifras proporcionalmente similares a la estructura de mercado de la telefonía móvil [62]. *[Ver figura15]*

[Figura 13] Datos obtenidos a partir de respuestas a solicitudes de acceso a la información pública realizadas a la Procuraduría General de la República.

[Figura 14] Nota 1: Datos obtenidos a partir de respuestas a solicitudes de acceso a la información pública realizadas a autoridades federales y de las 32 entidades federativas. La Fiscalía General del Estado de Aguascalientes, la Procuraduría General de Justicia de la Ciudad de México y la Procuraduría General de Justicia del Estado de Guanajuato no entregaron información. La Fiscalía General del Estado de Chihuahua no entregó información respecto del año 2013 y la Comisión Federal de Competencia Económica no entregó información respecto de 2015. Datos de reportes semestrales de transparencia enviados al Instituto Federal de Telecomunicaciones por Alestra, AT&T, Axtel, BBG Comunicaciones, IP Matrix, Marcatel, Maxcom, Megacable, Movistar y Telcel obtenidos a partir de una solicitud de acceso a la información. El número total de autoridades no se conoce con precisión dado que algunas compañías no identificaron a todas las autoridades solicitantes.

[62] Para el cuarto trimestre del 2015 Telcel contaba con 68% del mercado de telefonía móvil, Movistar 23.1% y AT&T un 8.1%. Esto según datos del Cuarto Informe Trimestral Estadístico del IFT. Disponible en: http://www.ift.org.mx/sites/default/files/comunicacion-y-medios/informes/informetrimestral4q2015versionhabilitadaparalectordepantallav3.pdf

[Figura 15] Datos de reportes semestrales de transparencia enviados al Instituto Federal de Telecomunicaciones por Alestra, AT&T, Axtel, BBG Comunicaciones, IP Matrix, Marcatel, Maxcom, Megacable, Movistar y Telcel obtenidos a partir de una solicitud de acceso a la información.

Figura 14

NÚMERO DE AUTORIDADES QUE SOLICITARON ACCESO A DATOS CONSERVADOS POR EMPRESAS DE TELECOMUNICACIONES

2013-2015 · SAI - REPORTES A IFT

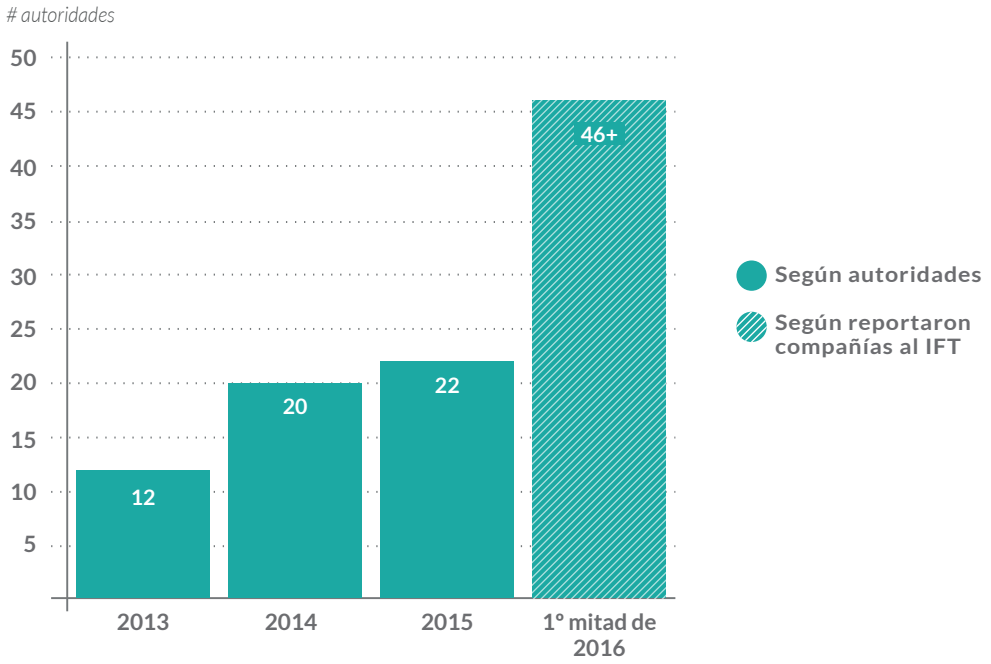
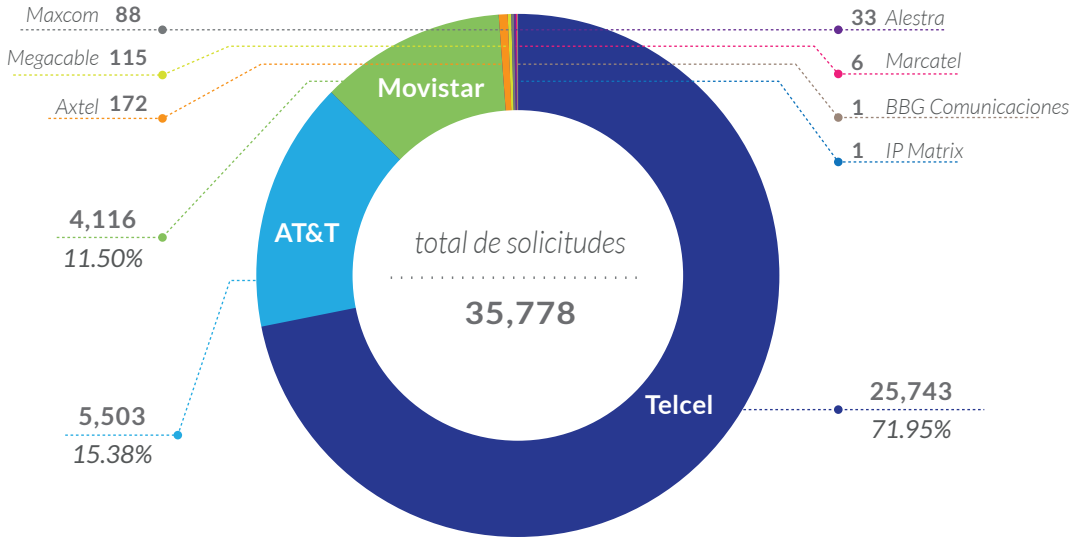


Figura 15

SOLICITUDES DE ACCESO A DATOS CONSERVADOS RECIBIDAS POR EMPRESAS DE TELECOMUNICACIONES

1ER SEMESTRE DE 2016 - REPORTES A IFT



La PGR y otras fiscalías y procuradurías como las de Veracruz, Ciudad de México, Guanajuato, Estado de México y Chihuahua fueron las autoridades que más solicitudes realizaron en el primer semestre de 2016 además de las que provienen del Poder Judicial de la Federación. Algunas empresas, en particular Telcel, no revelaron la identidad de autoridades que realizaron una gran cantidad de solicitudes recibidas. *[Ver figura 16]*

Las empresas de telecomunicaciones únicamente rechazaron 2966 de las 35778 solicitudes recibidas, es decir, apenas el 8.29%. *[Ver figura 17]*

La empresa que más solicitudes rechazó fue AT&T con 63.5% de las solicitudes recibidas, seguido de Megacable (servicios fijos) con 46.6% y Movistar que rechazó el 8% de las solicitudes de acceso a datos de usuarios. Es altamente preocupante que Telcel no haya rechazado ni una sola solicitud de ADC en el primer semestre de 2016, siendo la empresa que recibe la mayor cantidad de de parte de autoridades. *[Ver figura 18]*

Un análisis detallado de la información entregada al IFT por las empresas de telecomunicaciones revela que una gran cantidad de autoridades que no poseen facultad legal o constitucional para llevar a cabo solicitudes de ADC lo hicieron, peor aún, en una cantidad muy importante de ocasiones los datos de los usuarios fueron entregados. *[Ver figura 19]*

[Figura 16] Datos de reportes semestrales de transparencia enviados al Instituto Federal de Telecomunicaciones por Alestra, AT&T, Axtel, BBG Comunicaciones, IP Matrix, Marcatel, Maxcom, Megacable, Movistar y Telcel obtenidos a partir de una solicitud de acceso a la información. Algunas compañías no identificaron a todas las autoridades solicitantes.

[Figura 17] Datos de reportes semestrales de transparencia enviados al Instituto Federal de Telecomunicaciones por Alestra, AT&T, Axtel, BBG Comunicaciones, IP Matrix, Marcatel, Maxcom, Megacable, Movistar y Telcel obtenidos a partir de una solicitud de acceso a la información.

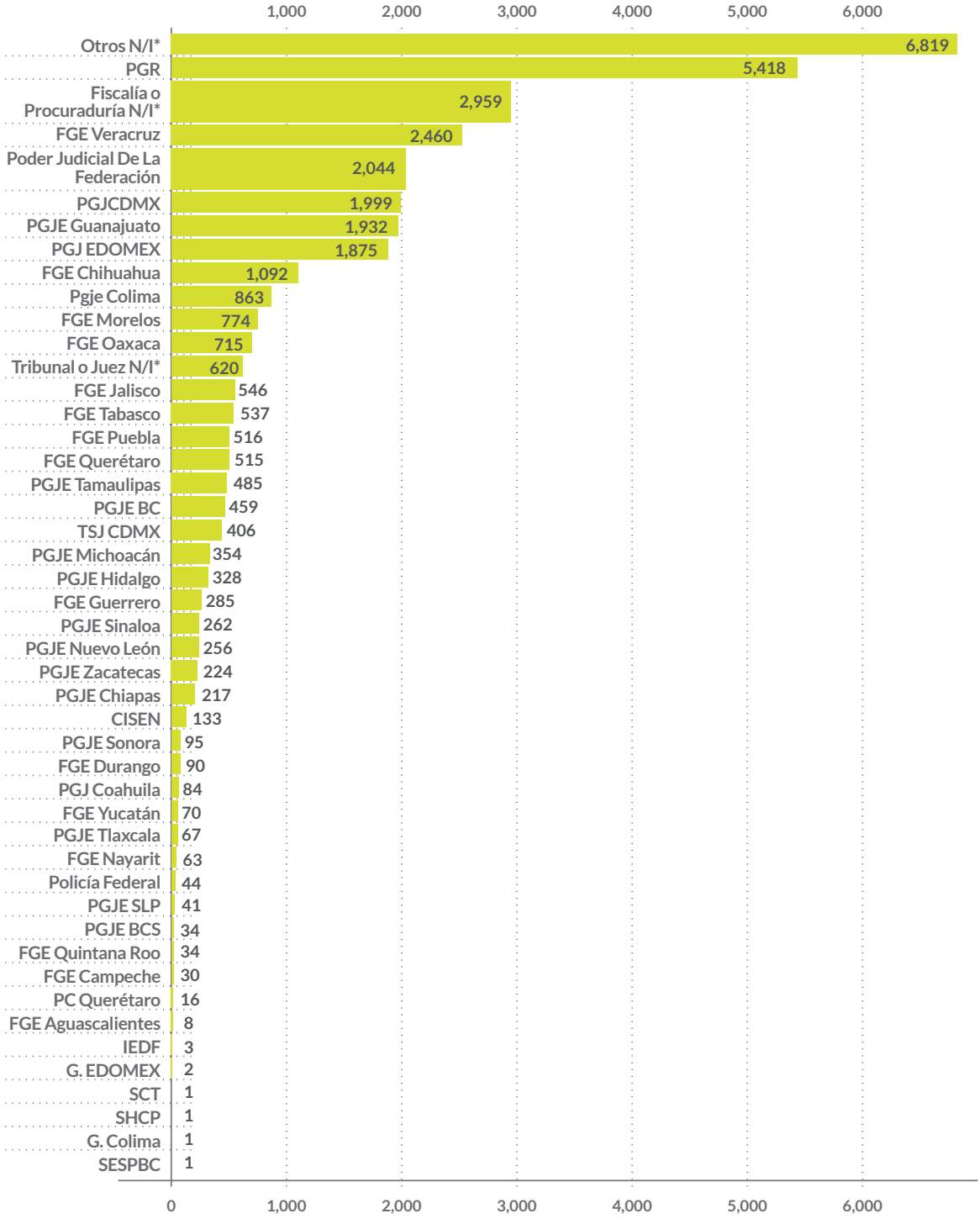
[Figura 18] Datos de reportes semestrales de transparencia enviados al Instituto Federal de Telecomunicaciones por Alestra, AT&T, Axtel, BBG Comunicaciones, IP Matrix, Marcatel, Maxcom, Megacable, Movistar y Telcel obtenidos a partir de una solicitud de acceso a la información. Las compañías que no aparecen en la gráfica no rechazaron ninguna solicitud.

[Figura 19] Datos de reportes semestrales de transparencia enviados al Instituto Federal de Telecomunicaciones por Alestra, AT&T, Axtel, BBG Comunicaciones, IP Matrix, Marcatel, Maxcom, Megacable, Movistar y Telcel obtenidos a partir de una solicitud de acceso a la información. Algunas compañías no identificaron a todas las autoridades solicitantes.

Figura 16

SOLICITUDES DE ACCESO A DATOS CONSERVADOS RECIBIDAS POR EMPRESAS DE TELECOMUNICACIONES

1ER SEMESTRE DE 2016 - REPORTES A IFT



* N/I = No Identificado

Totales Solicitudes 35,778

Figura 17

SOLICITUDES DE ACCESO A DATOS CONSERVADOS RECIBIDAS POR EMPRESAS DE TELECOMUNICACIONES % DE RECHAZO

1ER SEMESTRE DE 2016 - REPORTES A IFT

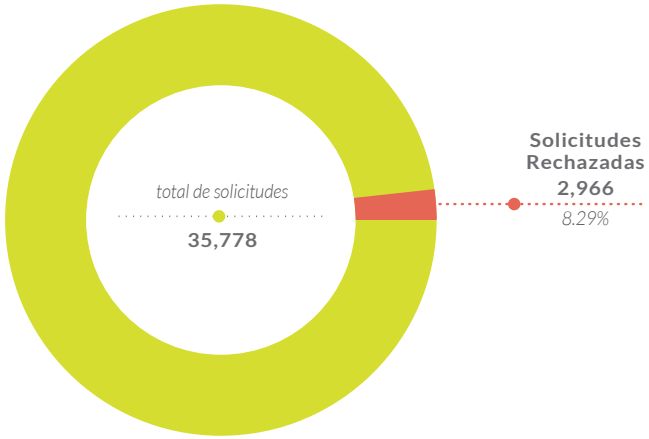


Figura 18

SOLICITUDES DE ACCESO A DATOS CONSERVADOS RECIBIDAS POR EMPRESAS DE TELECOMUNICACIONES % DE RECHAZO POR COMPAÑÍA

1ER SEMESTRE DE 2016 - REPORTES A IFT

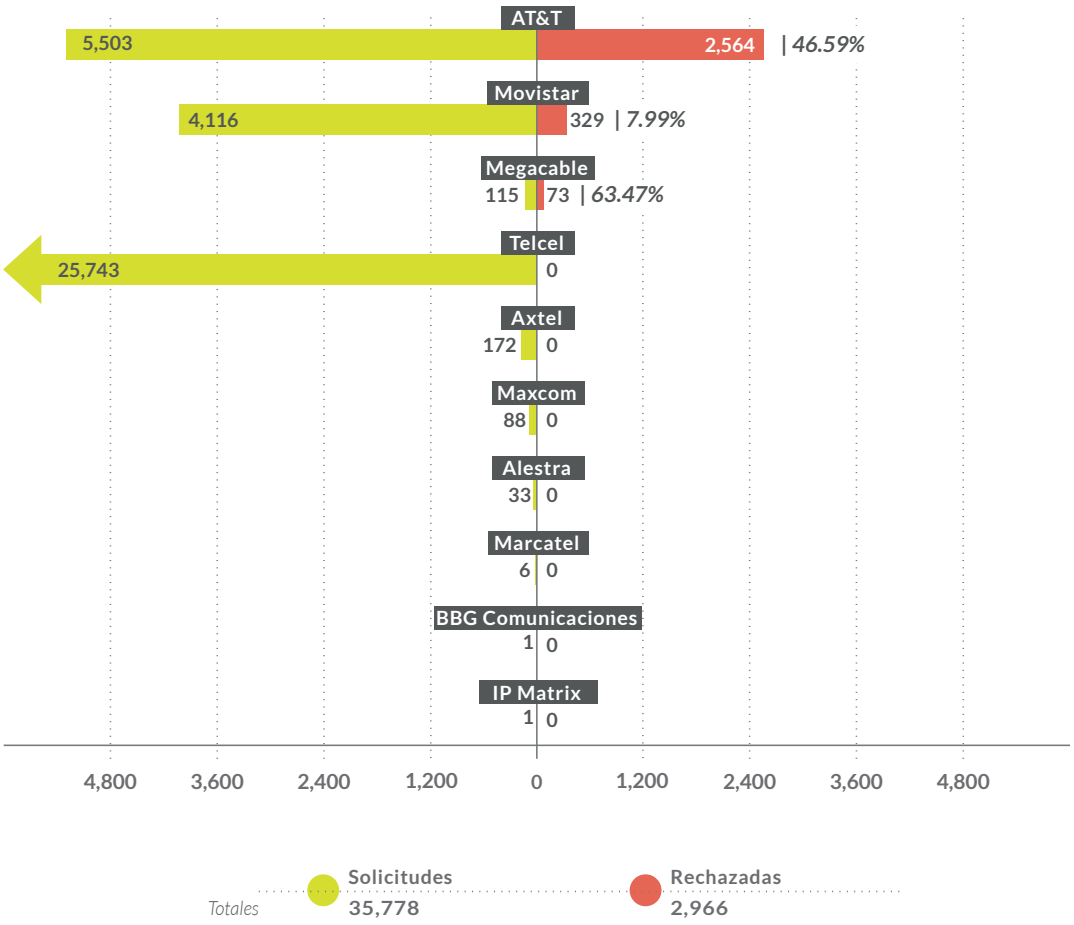
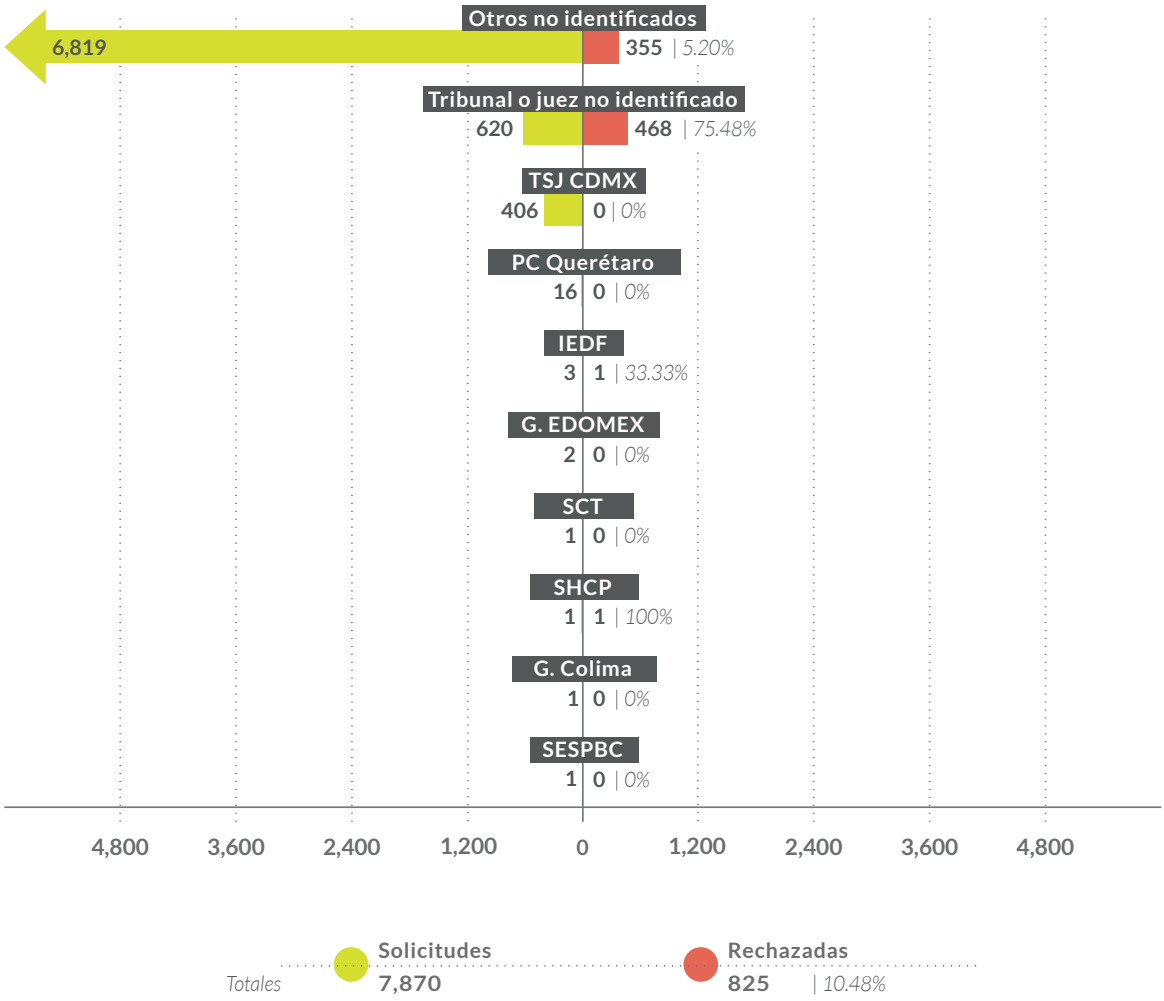


Figura 19

SOLICITUDES DE ACCESO A DATOS CONSERVADOS RECIBIDAS POR EMPRESAS DE TELECOMUNICACIONES DE PARTE DE AUTORIDADES NO FACULTADAS
% DE RECHAZO
1ER SEMESTRE DE 2016 - REPORTES A IFT



5.3 GEOLOCALIZACIÓN EN TIEMPO REAL

El monitoreo de la localización geográfica en tiempo real de equipos de comunicación móvil (geolocalización), es una medida de vigilancia que aparentemente ha sido utilizada en un volumen menor al de otras medidas de vigilancia.

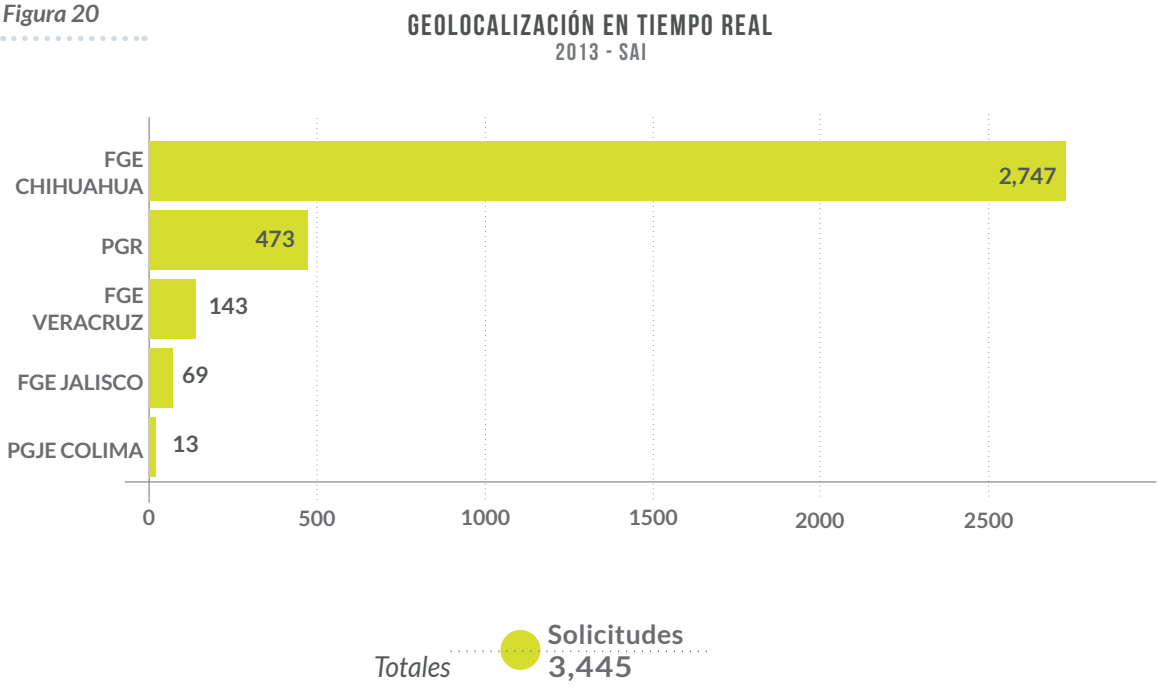
De 2013 a 2015 se ha documentado su utilización en 11994 ocasiones. En 2013 se realizaron 3445 solicitudes. En 2014, el número ascendió a 4324 y en 2015 fueron

4225 las veces en las que una autoridad solicitó la colaboración de una empresa para llevar a cabo la geolocalización en tiempo real.

Llama la atención que durante los años 2013 a 2015, la Fiscalía General del Estado de Chihuahua (FGE Chihuahua) haya sido la autoridad que, por mucho, intentó obtener la geolocalización de un dispositivo en más ocasiones. Fueron **2747 las veces en las que FGE Chihuahua envió solicitudes de geolocalización en 2013**. Casi el 80% de todas las solicitudes de ese año. La FGE Chihuahua se mantuvo a la cabeza en los años 2014 y 2015, con 1941 y 1986 solicitudes respectivamente.

La PGR y la Fiscalía General del Estado de Veracruz (FGE Veracruz) **fueron las autoridades que más solicitaron la geolocalizació**n de usuarios de telecomunicaciones durante el periodo analizado. *[Ver figuras 20, 21 y 22]*

Figura 20



[Figura 20] Datos obtenidos a partir de respuestas a solicitudes de acceso a la información pública realizadas a autoridades federales y de las 32 entidades federativas. La Fiscalía General del Estado de Aguascalientes, la Fiscalía General del Estado de Quintana Roo, la Procuraduría General de Justicia de la Ciudad de México y la Procuraduría General de Justicia del Estado de Guanajuato no entregaron información.

[Figura 21] Datos obtenidos a partir de respuestas a solicitudes de acceso a la información pública realizadas a autoridades federales y de las 32 entidades federativas. La Fiscalía General del Estado de Aguascalientes, la Procuraduría General de Justicia de la Ciudad de México y la Procuraduría General de Justicia del Estado de Guanajuato no entregaron información.

[Figura 22] Datos obtenidos a partir de respuestas a solicitudes de acceso a la información pública realizadas a autoridades federales y de las 32 entidades federativas. La Fiscalía General del Estado de Aguascalientes, la Procuraduría General de Justicia del Estado de Chiapas, la Procuraduría General de Justicia de la Ciudad de México y la Procuraduría General de Justicia del Estado de Guanajuato no entregaron información.

Figura 21

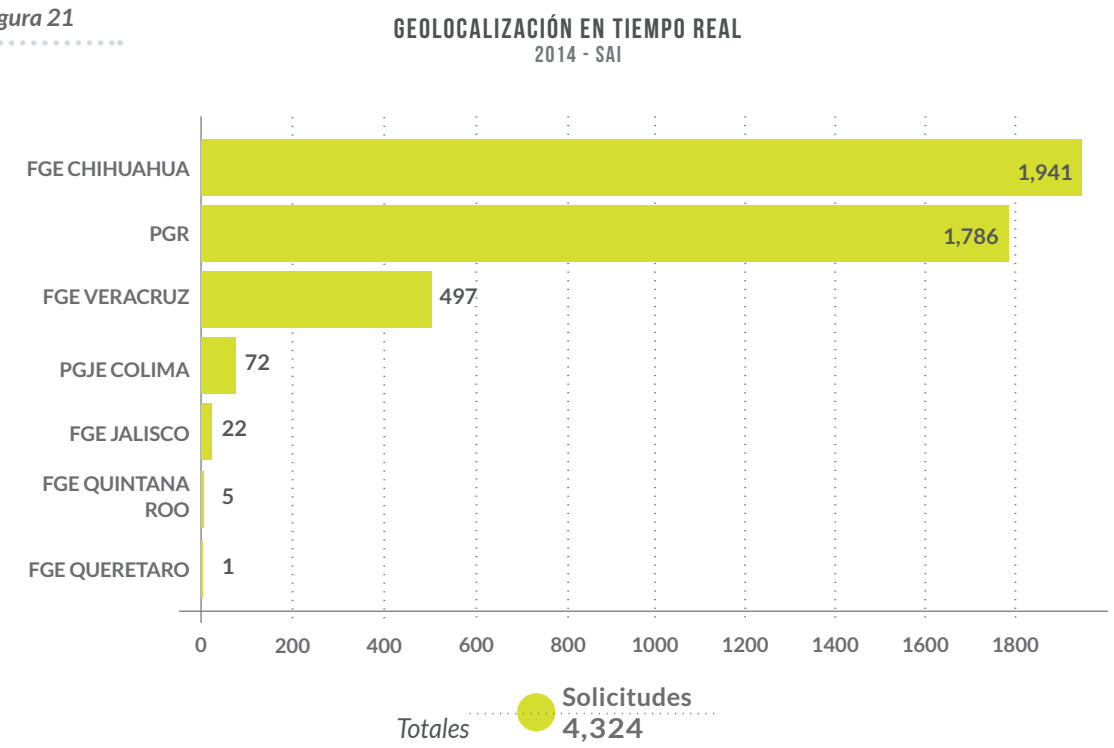
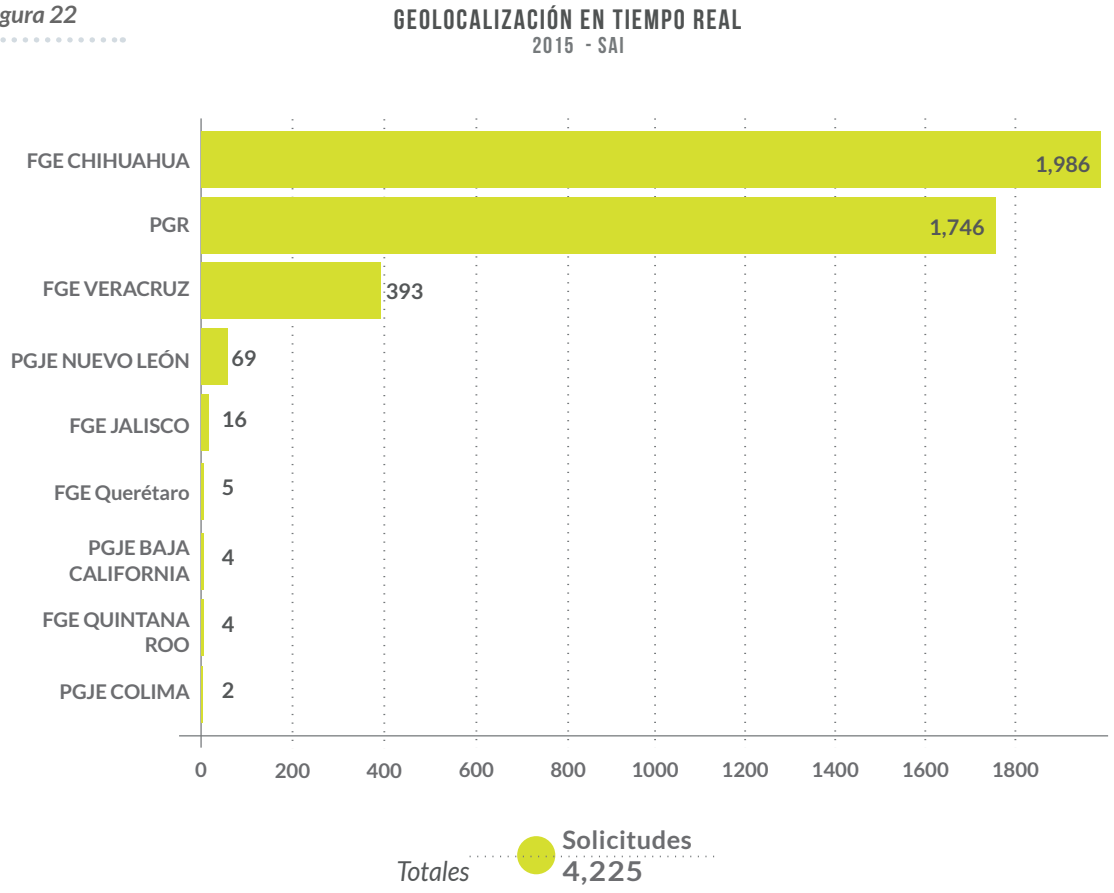


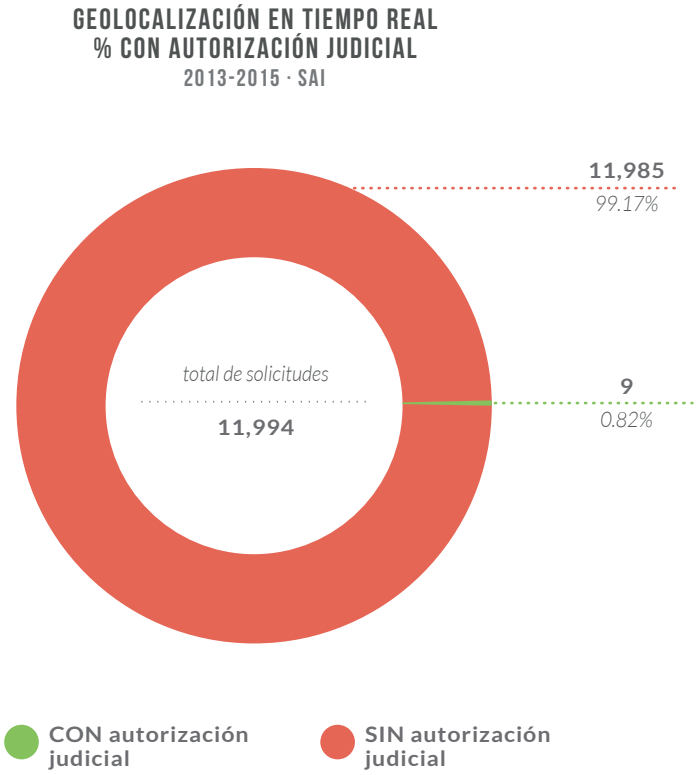
Figura 22



Prácticamente la totalidad de las solicitudes de geolocalización en tiempo real realizadas entre 2013 y 2015 fueron llevadas a cabo sin autorización judicial. Únicamente el 0.82% sí contaron con dicha autorización a solicitud de la Fiscalía General del Estado de Quintana Roo.

Si bien durante esos años la ley no exigía la autorización judicial, es importante resaltar el artículo 303 del Código Nacional de Procedimientos Penales vigente ya lo exige, salvo casos de emergencia en los que, de cualquier manera, debe darse aviso al juez.

Figura 23

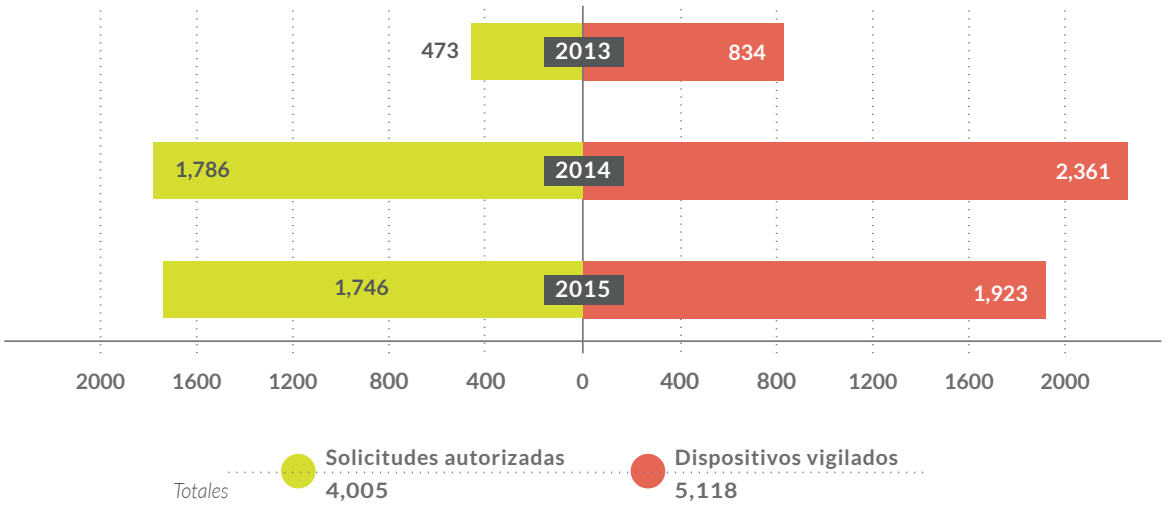


En el caso de la geolocalización en tiempo real, también se observa que el número de solicitudes no es equivalente al número de equipos vigilados. Por ejemplo, según la PGR, esa autoridad llevó a cabo 4005 geolocalizaciones entre 2013 y 2015, sin embargo monitoreó la localización de 5118 dispositivos. *[Ver figura 24]*

[Figura 23] Datos obtenidos a partir de respuestas a solicitudes de acceso a la información pública realizadas a autoridades federales y de las 32 entidades federativas. La Fiscalía General del Estado de Aguascalientes, la Procuraduría General de Justicia de la Ciudad de México y la Procuraduría General de Justicia del Estado de Guanajuato no entregaron información. La Fiscalía General del Estado de Quintana Roo no entregó información respecto del año 2013 y la Procuraduría General de Justicia del Estado de Chiapas no entregó información respecto de 2015. Las 9 solicitudes que sí contaron con autorización judicial fueron realizadas por la Fiscalía General del Estado de Quintana Roo.

Figura 24

NÚMERO DE SOLICITUDES DE GEOLOCALIZACIÓN EN TIEMPO REAL VS DISPOSITIVOS VIGILADOS (PGR)
2013-2015 · SAI



De igual manera que respecto de otras medidas de vigilancia, el número de autoridades que se ha documentado que solicitan la geolocalización en tiempo real ha ido aumentando de manera constante. En 2013 se documentaron cinco autoridades, en 2014 fueron 7 y en 2015 fueron nueve las autoridades que utilizaron esta medida de vigilancia.

No obstante lo anterior, los informes semestrales remitidos por las empresas de telecomunicaciones al IFT revelan que, en el primer semestre de 2016, al menos 21 autoridades solicitaron una geolocalización en tiempo real, por lo tanto, es posible que el número de autoridades que hicieron uso de esta facultad entre 2013 y 2015 sea mayor o, con menor probabilidad, que en 2016 haya habido un incremento exponencial de este tipo de solicitudes. *[Ver figura 25]*

Únicamente tres empresas reportaron haber recibido solicitudes de geolocalización en tiempo real en el primer semestre de 2016. La compañía que más solicitudes recibió fue Telcel, con 1929. Movistar recibió 225 y AT&T recibió 170. *[Ver figura 26]*

[Figura24] Datos obtenidos a partir de respuestas a solicitudes de acceso a la información pública realizadas a la Procuraduría General de la República.

[Figura 25] Datos obtenidos a partir de respuestas a solicitudes de acceso a la información pública realizadas a autoridades federales y de las 32 entidades federativas. La Fiscalía General del Estado de Aguascalientes, la Procuraduría General de Justicia de la Ciudad de México y la Procuraduría General de Justicia del Estado de Guanajuato no entregaron información. La Fiscalía General del Estado de Quintana Roo no entregó información respecto del año 2013 y la Procuraduría General de Justicia del Estado de Chiapas no entregó información respecto de 2015. Datos de reportes semestrales de transparencia enviados al Instituto Federal de Telecomunicaciones por Alestra, AT&T, Axtel, BBG Comunicaciones, IP Matrix, Marcatel, Maxcom, Megacable, Movistar y Telcel obtenidos a partir de una solicitud de acceso a la información. El número total de autoridades no se conoce con precisión dado que algunas compañías no identificaron a todas las autoridades solicitantes.

Figura 25

NÚMERO DE AUTORIDADES QUE SOLICITARON GEOLOCALIZACIÓN EN TIEMPO REAL

2013-2015 - SAI - REPORTES A IFT

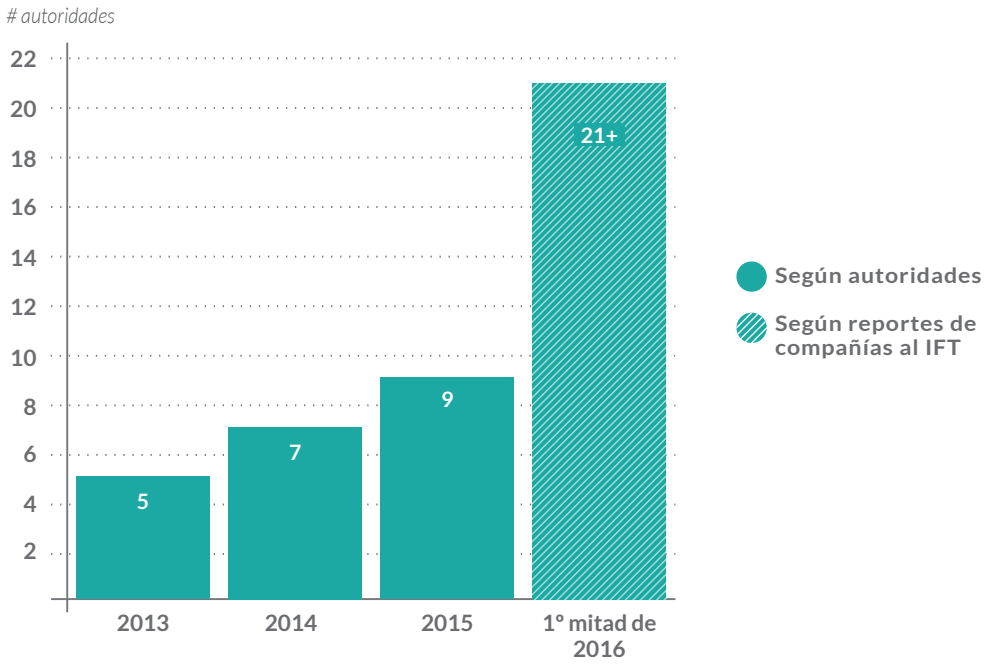
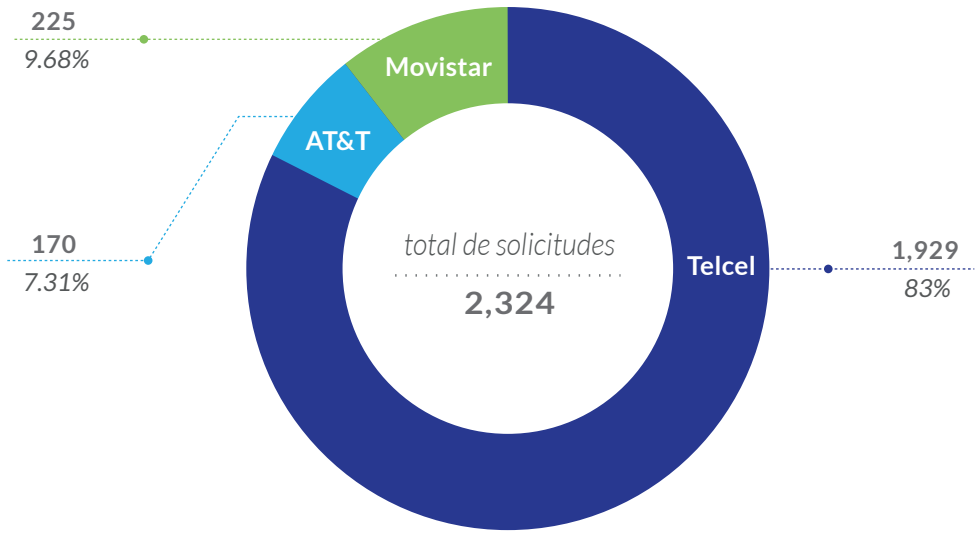


Figura 26

SOLICITUDES DE GEOLOCALIZACIÓN EN TIEMPO REAL POR COMPAÑÍA

1ER SEMESTRE DE 2016 - REPORTES A IFT



La PGR aparece como la autoridad que más veces solicitó la geolocalización en tiempo real en el primer semestre de 2016 con 954, seguido de la FGE Veracruz, con 322 y la PGJ CDMX con 290.

Es de resaltar que ninguna compañía reporte haber recibido una sola solicitud de la FGE Chihuahua, cuando durante los años 2013 a 2015 fue la autoridad respecto de la cual se encuentra documentada la mayor cantidad de solicitudes. Esta anomalía es difícil de explicar y puede sugerir que la FGE Chihuahua esté llevando a cabo el monitoreo de la geolocalización de dispositivos de comunicación a través de métodos que no requieren la colaboración de las empresas de telecomunicaciones, lo cual, en su caso, sería muy cuestionable desde el punto de vista legal.

A diferencia de las solicitudes de ADC no se ha detectado que alguna autoridad que haya solicitado la geolocalización en tiempo real no tenga, en principio, la facultad legal para hacer la solicitud, aunque **Telcel omitió identificar a autoridades que hicieron algunas solicitudes de geolocalización**, por lo que la posibilidad de que alguna autoridad sin facultades legales haya monitoreado la geolocalización de alguna persona no puede descartarse. *[Ver figura 27]*

En el primer semestre de 2016, únicamente 32 solicitudes de geolocalización fueron rechazadas por alguna compañía de un total de 2324; el equivalente al 1.37% del total de solicitudes recibidas. *[Ver figura 28]*

De nueva cuenta, los informes semestrales remitidos por las empresas de telecomunicaciones al IFT revelan que **Telcel no rechazó ninguna solicitud de geolocalización recibida.** En cambio, AT&T rechazó el 10% y Movistar el 6.66% de las solicitudes recibidas.

La ausencia de instancias en las que Telcel haya rechazado alguna solicitud de alguna medida de vigilancia, levanta serias dudas respecto de si esa compañía lleva a cabo algún procedimiento de revisión legal de las solicitudes que impida el acceso ilegal a los datos de sus usuarios. *[Ver figura 29]*

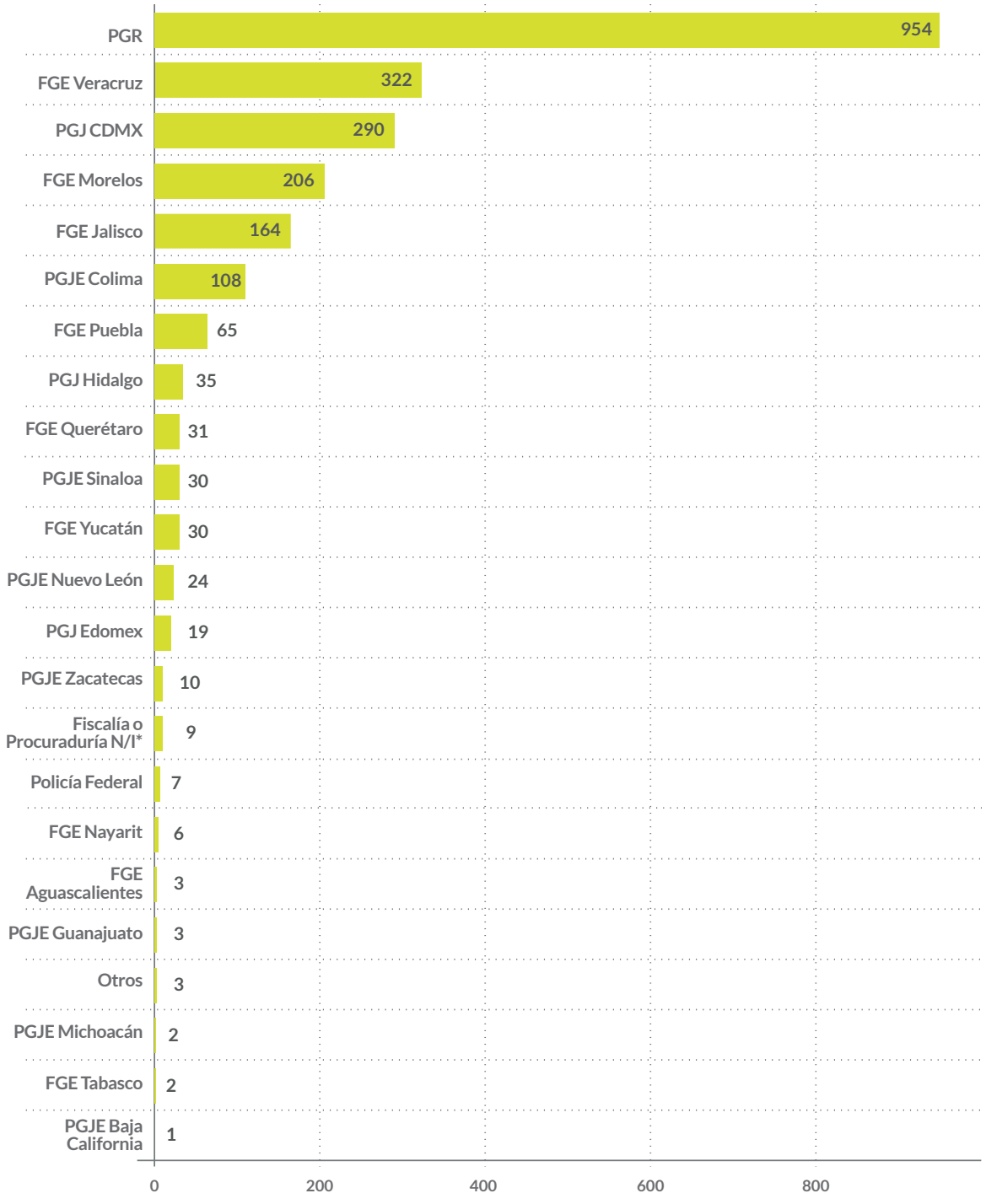
[Figura 26] Nota: Datos de reportes semestrales de transparencia enviados al Instituto Federal de Telecomunicaciones por Alestra, AT&T, Axtel, BBG Comunicaciones, IP Matrix, Marcatel, Maxcom, Megacable, Movistar y Telcel obtenidos a partir de una solicitud de acceso a la información.

[Figura 27] Datos de reportes semestrales de transparencia enviados al Instituto Federal de Telecomunicaciones por Alestra, AT&T, Axtel, BBG Comunicaciones, IP Matrix, Marcatel, Maxcom, Megacable, Movistar y Telcel obtenidos a partir de una solicitud de acceso a la información. Algunas compañías no identificaron a todas las autoridades solicitantes.

Figura 27

SOLICITUDES DE GEOLOCALIZACIÓN EN TIEMPO REAL POR AUTORIDAD

1ER SEMESTRE DE 2016 - REPORTES A IFT



Totales Solicitudes 14,129

Figura 28

SOLICITUDES DE GEOLOCALIZACIÓN EN TIEMPO REAL
% DE RECHAZO
1ER SEMESTRE DE 2016 - REPORTES A IFT

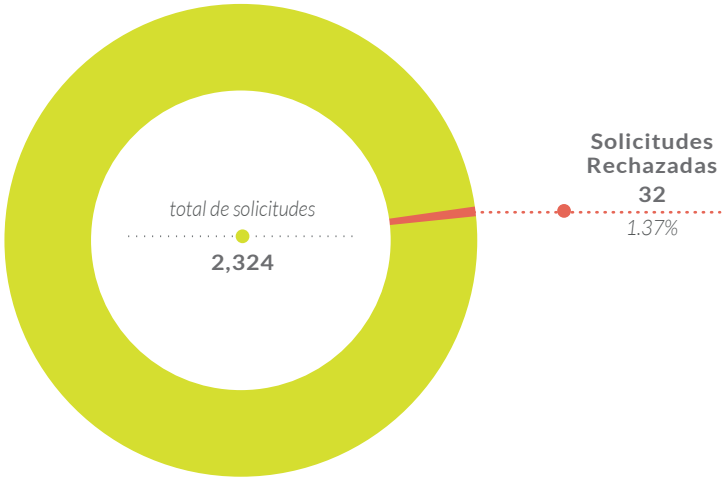
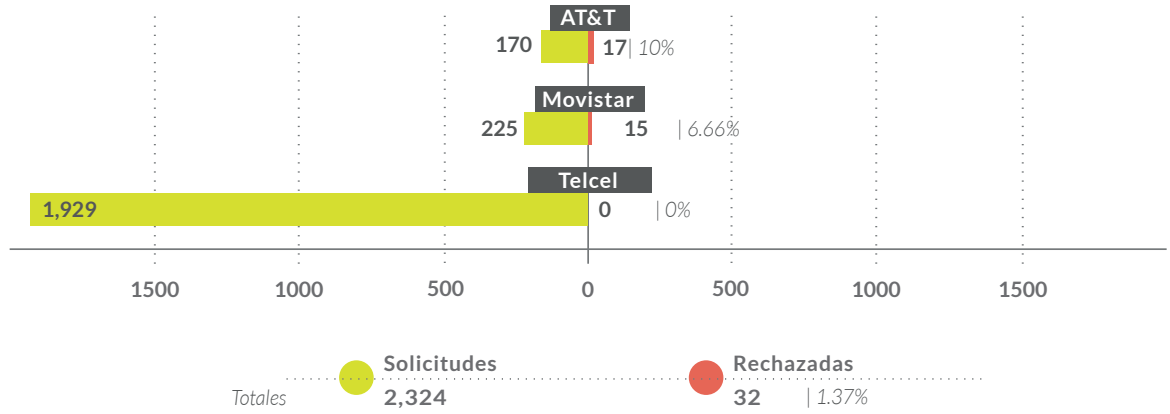


Figura 29

SOLICITUDES DE GEOLOCALIZACIÓN EN TIEMPO REAL RECHAZADAS
% POR COMPAÑÍA
1ER SEMESTRE DE 2016 - REPORTES A IFT



[Figura 28] Datos de reportes semestrales de transparencia enviados al Instituto Federal de Telecomunicaciones por Alestra, AT&T, Axtel, BBG Comunicaciones, IP Matrix, Marcatel, Maxcom, Megacable, Movistar y Telcel obtenidos a partir de una solicitud de acceso a la información.

[Figura 29] Datos de reportes semestrales de transparencia enviados al Instituto Federal de Telecomunicaciones por Alestra, AT&T, Axtel, BBG Comunicaciones, IP Matrix, Marcatel, Maxcom, Megacable, Movistar y Telcel obtenidos a partir de una solicitud de acceso a la información.

La geolocalización en tiempo real de un equipo de comunicación móvil, **implica el monitoreo continuo y, en ocasiones, prolongado de ese dispositivo**, lo cual a su vez fácilmente permite la identificación de la persona que lo utiliza y de una cantidad importante de datos sensibles sobre ella.

A partir de SAI se ha podido documentar el plazo máximo aplicado por algunas autoridades para el monitoreo continuo de la geolocalización de un usuario. Los datos obtenidos revelan que autoridades como la PGR únicamente llevan a cabo la geolocalización por un máximo de un mes, mientras que **otras autoridades como la Fiscalía General del Estado de Veracruz lo hacen hasta por seis meses** [63].

AUTORIDAD	PLAZO MÁXIMO DE GEOLOCALIZACIÓN
FGE Veracruz	6 meses
PGJE Baja California	3 meses
FGE Querétaro	3 meses
PGR	1 mes

5.4 EFECTIVIDAD DE LA VIGILANCIA

La expansión de las facultades legales y tecnológicas para implementar medidas de vigilancia sobre la población, ha descansado, en gran parte, bajo argumentos que sostienen que éstas herramientas son indispensables para alcanzar objetivos legítimos del Estado como lo son la la seguridad y el combate a la impunidad.

Bajo esa lógica no soportada en evidencia, también se ha intentado justificar la eliminación de contrapesos institucionales y controles democráticos mínimos a la vigilancia. Se ha argumentado que el control judicial y otras medidas encaminadas a detectar, prevenir y evitar abusos a través de la vigilancia, son obstáculos innecesarios a la celeridad (rapidez) y efectividad de investigaciones.

En aras de **aportar a esta discusión de manera informada y con evidencia**, preguntamos a las procuradurías y fiscalías del país datos sobre las averiguaciones previas en las que se han utilizado medidas de vigilancia y datos sobre el estado procesal de las mismas.

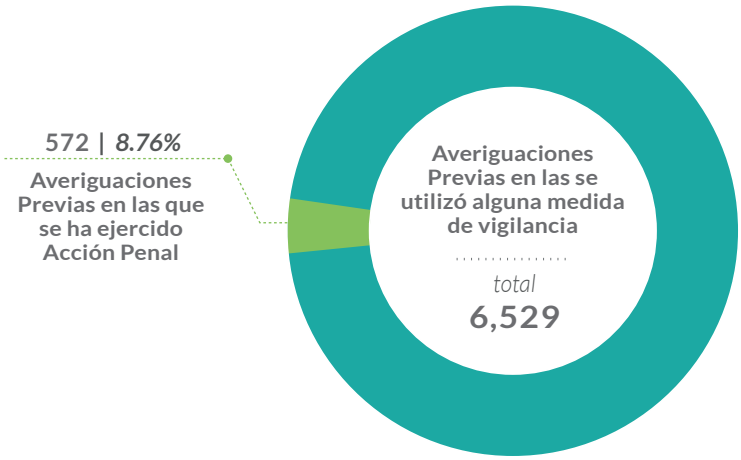
[63] Nota: Datos obtenidos a partir de respuestas a solicitudes de acceso a la información pública.

Si bien un número importante de procuradurías y fiscalías no aportaron la información solicitada o la aportaron de manera parcial. Los datos obtenidos demuestran que **la inmensa mayoría de las averiguaciones previas en las que se ha utilizado alguna medida de vigilancia no se ha ejercido acción penal alguna.** Únicamente el 8.76% de las averiguaciones previas en las que se utilizado alguna medida de vigilancia entre 2013 y 2015 se ha ejercido acción penal. Lo cual sugiere que aproximadamente el 90% de las personas que podrían haber sido vigiladas con fines de investigación penal no han sido acusadas de ningún delito ante un juez.

Figura 31

AVERIGUACIONES PREVIAS EN LAS QUE SE HA UTILIZADO ALGUNA MEDIDA DE VIGILANCIA (2013 - 2015) VS NÚMERO DE AVERIGUACIONES PREVIAS EN LAS QUE SE HA EJERCIDO ACCIÓN PENAL - TOTAL

2013-2015 - SAI



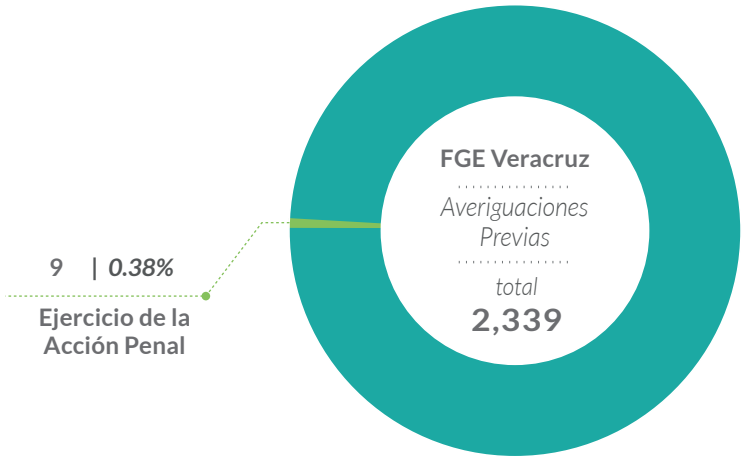
El caso de la FGE Veracruz son especialmente dramáticos. De 2339 averiguaciones previas en las que dicha autoridad señala que se han utilizado medidas de vigilancia, únicamente en 9 se ha ejercido acción penal. Es decir, sólo en el 0.38% la investigación ha culminado con una acusación penal en contra de alguna persona. *[Ver figura 32]*

[Figura 31] Datos obtenidos a partir de respuestas a solicitudes de acceso a la información pública realizadas a la PGR y las Procuradurías y Fiscalías de las 32 entidades federativas. La Procuraduría General de la República, la Fiscalía General del Estado de Aguascalientes, la Procuraduría General de Justicia del Estado de Baja California Sur, la Fiscalía General del Estado de Chihuahua, la Procuraduría General de Justicia de la Ciudad de México, la Procuraduría General de Justicia del Estado de México, la Procuraduría General de Justicia del Estado de Guanajuato, la Procuraduría General de Justicia del Estado de Michoacán, la Fiscalía General del Estado de Morelos, la Fiscalía General del Estado de Nayarit, la Procuraduría General de Justicia del Estado de Sinaloa y la Fiscalía General del Estado de Yucatán no entregaron información.

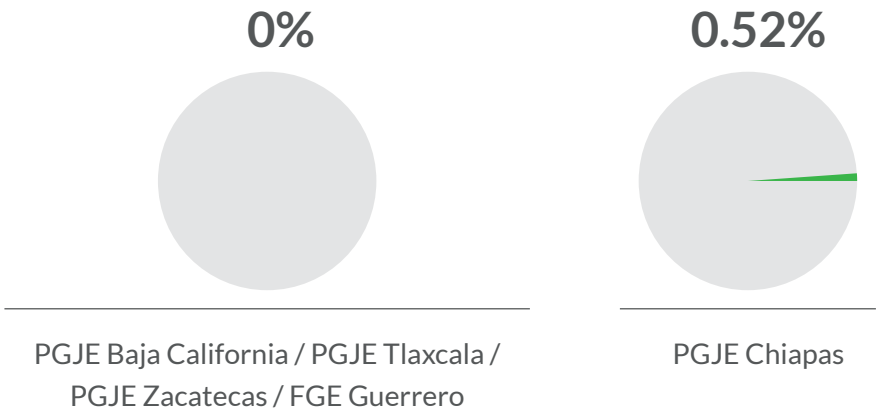
Figura 32

AVERIGUACIONES PREVIAS EN LAS QUE SE HA UTILIZADO ALGUNA MEDIDA DE VIGILANCIA (2013 - 2015) VS NÚMERO DE AVERIGUACIONES PREVIAS EN LAS QUE SE HA EJERCIDO ACCIÓN PENAL - FGE VERACRUZ

2013-2015 - SAI



En el caso de las PGJE de Baja California, PGJE Tlaxcala, PGJE Zacatecas y FGE Guerrero en ninguna Averiguación Previa en donde se ha utilizado alguna medida de vigilancia se ha ejercido acción penal. En el caso de PGJE de Chiapas, únicamente en 1 Averiguación Previa de 189, es decir, en el 0.52%, se ha ejercido acción penal.



Porcentaje de Averiguaciones Previas en el que se ha usado alguna medida de vigilancia y se ha ejercido acción penal [64]

[Figura 32] Datos obtenidos a partir de respuestas a solicitudes de acceso a la información pública realizadas a la FGE Veracruz.
[64] Datos obtenidos a partir de respuestas a solicitudes de acceso a la información pública.

Inclusive en los Estados en los que la tasa de ejercicio de la acción penal es mayor, como FGE Quintana Roo (38.6%), PGJE Tabasco (24.3%) y FGE Jalisco (21.57%), al menos el 61% de las averiguaciones previas en las que se ha utilizado alguna medida de vigilancia permanecen abiertas, han concluído sin acusación o se ha tomado una determinación distinta al ejercicio de la acción penal. *[Ver figura 33]*

Estos datos revelan, por un lado, que en el mejor de los casos la utilidad y eficacia de las medidas de vigilancia para fines de investigación criminal ha sido exagerada y, más preocupante, que en una gran cantidad de casos **las autoridades investigadoras utilizan herramientas de vigilancia en contra de personas respecto de las cuales no existe evidencia de que hayan participado en la comisión de un delito.** Este hecho, aunado a que el ejercicio de una gran cantidad de medidas de vigilancia fue llevado a cabo sin control judicial y sin la existencia de otras salvaguardas, sugiere en gran medida que la vigilancia estatal podría haber sido utilizada de manera ilegítima en contra de personas de manera impune.

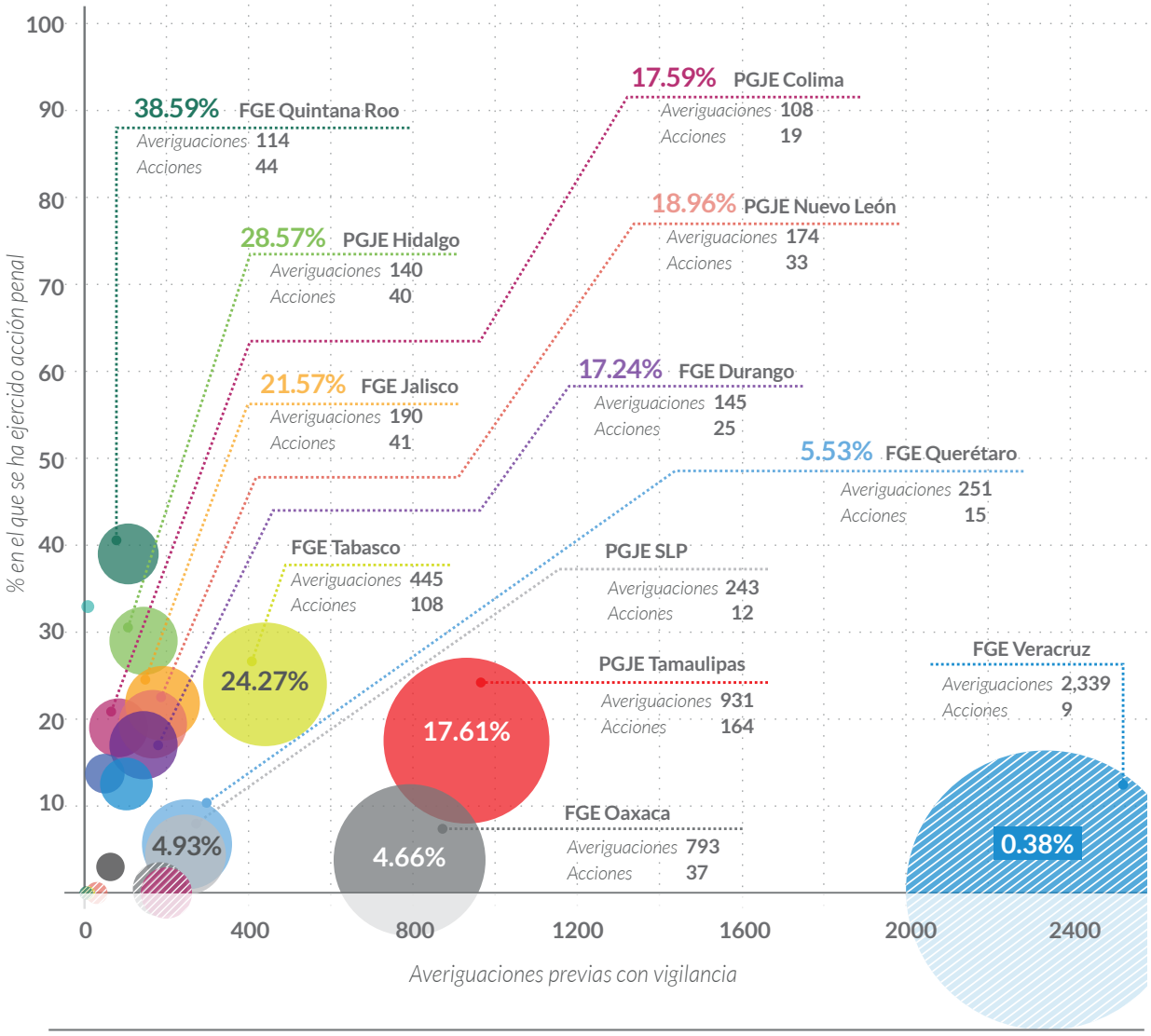
De esta forma, resultaría sumamente difícil seguir sosteniendo la tesis de que la vigilancia, en automático, equivale a investigaciones eficaces. Pero además, resulta innegable que, ante la evidencia presentada sobre cómo las medidas de vigilancia han sido utilizadas en la práctica, existen grandes incentivos para utilizar la vigilancia de manera ilegal, incluso arriesgando la propia seguridad de la ciudadanía que los proponentes de la vigilancia sin controles dicen proteger.

[Figura 33] Datos obtenidos a partir de respuestas a solicitudes de acceso a la información pública realizadas a la PGR y las Procuradurías y Fiscalías de las 32 entidades federativas. La Procuraduría General de la República, la Fiscalía General del Estado de Aguascalientes, la Procuraduría General de Justicia del Estado de Baja California Sur, la Fiscalía General del Estado de Chihuahua, la Procuraduría General de Justicia de la Ciudad de México, la Procuraduría General de Justicia del Estado de México, la Procuraduría General de Justicia del Estado de Guanajuato, la Procuraduría General de Justicia del Estado de Michoacán, la Fiscalía General del Estado de Morelos, la Fiscalía General del Estado de Nayarit, la Procuraduría General de Justicia del Estado de Sinaloa y la Fiscalía General del Estado de Yucatán no entregaron información.

Figura 33

AVERIGUACIONES PREVIAS EN LAS QUE SE HA UTILIZADO ALGUNA MEDIDA DE VIGILANCIA VS NÚMERO DE AVERIGUACIONES PREVIAS EN LAS QUE SE HA EJERCIDO ACCIÓN PENAL

2013-2015 - SAI

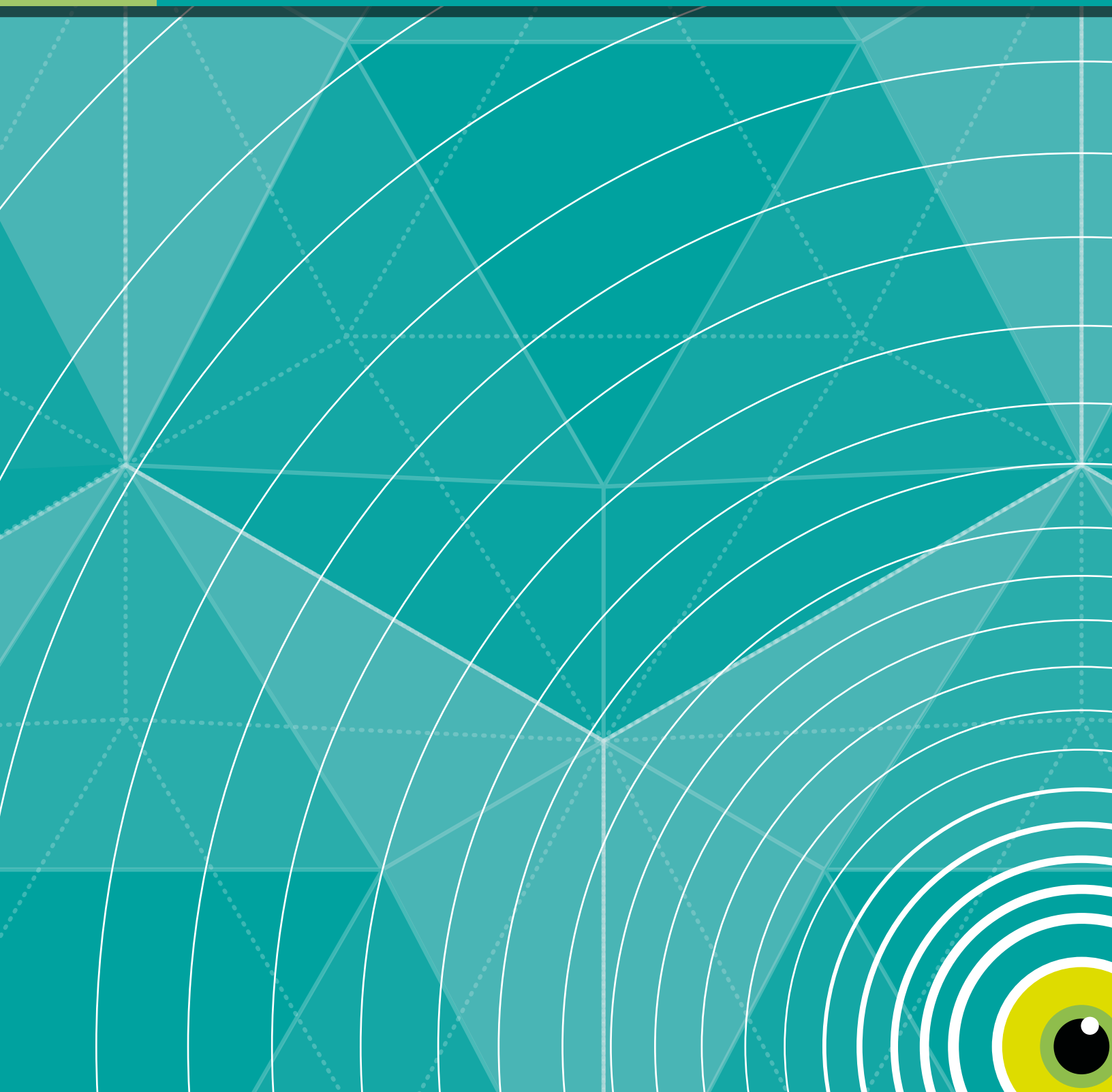


	Averiguaciones	Acciones	%
PGJE Tlaxcala	198	0	0%
PGJE Zacatecas	30	0	0%
PGJE BC	8	0	0%
FGE Guerrero	6	0	0%
PGJE Chiapas	189	1	0.52%

	Averiguaciones	Acciones	%
FGE Campeche	63	2	3.17%
PGJE Sonora	104	13	12.50%
FGE Puebla	55	8	14.54%
PGJE Coahuila	3	1	33.33%

Nota metodológica: Se realizaron solicitudes de acceso a la información a: CISEN, COFECE, INE, PGR, Secretaría de Marina, Secretaría de la Defensa Nacional, SHCP, Policía Federal, al CJF, al Gobierno del Estado de Aguascalientes, Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública de Aguascalientes, Secretaría de Gobierno de Aguascalientes, Oficina del Despacho de Gobierno de Aguascalientes, y a la FGE Aguascalientes. Oficina del Titular del Ejecutivo de Baja California, Secretaría General de Gobierno del Estado de Baja California, Secretaría de Seguridad Pública del Estado de Baja California y FGE de Baja California. Oficina del Gobernador de Baja California Sur, Secretaría de Gobernación del Estado de Baja California Sur, Secretaría de Gobernación del Estado de Baja California Sur, Policía Estatal de Baja California Sur, y a la PGJE Baja California Sur. Secretaría de Gobierno de Campeche, Secretaría de Seguridad Pública y Protección a la Comunidad del Estado de Campeche, Consejo Estatal de Seguridad Pública en el Estado de Campeche, Secretaría de Gobierno de Campeche, y FGE Campeche. Oficina del Gobernador de Chiapas, Secretaría de Seguridad y Protección Ciudadana del Estado de Chiapas, Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública del Estado de Chiapas, y PGJE Chiapas. Secretaría General de Gobierno de Chihuahua, Despacho del Gobernador de Chihuahua, y FGE Chihuahua. Comisión de Seguridad de Coahuila, Oficina del Gobierno de Coahuila, Secretaría de Gobierno de Coahuila, PGJE Coahuila. Jefatura De Gobierno de la Ciudad de México, Secretaría de Gobierno de la Ciudad de México, Secretaría de Seguridad Pública de la Ciudad de México, Policía Auxiliar de la Ciudad de México, Policía Bancaria e Industrial de la Ciudad de México, y PGJE Ciudad de México. Secretaría de Seguridad del Estado de Colima, Secretaría de Gobernación de Colima, Policía Estatal de Colima, Oficina del Gobernador del Estado de Colima, PGJE Colima. Oficina del Gobernador de Durango, Secretaría de Gobernación de Durango, Policía Estatal de Durango, y FGE de Durango. Gubernatura del Estado de México, Secretaría de Seguridad Ciudadana del Estado de México, y PGJE Estado de México. Secretaría de Gobierno del Estado de Guanajuato, Secretaría Particular del Gobernador del Estado de Guanajuato, Secretaría de Seguridad Pública del Estado de Guanajuato, PGJE Guanajuato. Secretaría de Seguridad Pública del Estado de Guerrero, Secretaría General de Gobierno del Estado de Guerrero, Secretaría Particular del C. Gobernador del Estado de Guerrero, y FGE Guerrero. Secretaría de Seguridad Pública del Estado de Hidalgo, Secretaría de Gobernación del Estado de Hidalgo, Policía Estatal de Hidalgo, Oficina del Gobernador de Hidalgo, y PGJE Hidalgo. FGE Jalisco. Secretaría de Gobernación del Estado de Michoacán, Secretaría de Seguridad Pública del Estado de Michoacán, Oficina del Gobernador del Estado de Michoacán, y PGJE Michoacán. Gubernatura del Estado de Morelos, Secretaría de Gobierno de Morelos, Policía Estatal de Morelos, Oficina del Gobernador del Estado de Morelos, y FGE Morelos. Secretaría de Seguridad Pública de Nayarit, Secretaría General del Gobierno del Estado de Nayarit, Oficina del Gobernante del Estado de Nayarit, Policía Estatal de Nayarit y FGE Nayarit. PGJE Nuevo León. FGE Oaxaca. Oficina del Gobernador del Estado de Puebla, Secretaría de Seguridad Pública de Puebla, Secretaría General del Estado de Puebla, FGE de Puebla. Secretaría de Gobierno de Querétaro, Oficina del Gobernador del Estado de Querétaro, Secretaría de Seguridad Pública de Querétaro, y FGE de Querétaro. Secretaría de Gobernación del Estado de Quintana Roo, Secretaría de Seguridad Pública del Estado de Quintana Roo, Oficina del Gobernador de Quintana Roo, y FGE Quintana Roo. Secretaría de Seguridad Pública de San Luis Potosí, Secretaría General de Gobernación del Estado de Quintana Roo, Secretaría Particular del Gobernador del Estado de Quintana Roo, FGE Quintana Roo. Oficina del Gobernador del Estado de Sinaloa, Secretaría de Seguridad Pública de Sinaloa, Secretaría General de Gobierno del Estado de Sinaloa, y PGJE Sinaloa. PGJE Sonora. FGE de Tabasco. PGJE Tamaulipas. Despacho del Gobernador del Estado de Tlaxcala, Secretaría de Gobierno del Estado de Tlaxcala, y PGJE Tlaxcala. Oficina del C. Gobernador del Estado de Veracruz, Secretaría de Gobernación del Estado de Veracruz, Secretaría de Seguridad Pública del Estado de Veracruz, y FGE Veracruz. FGE Yucatán. Jefatura de Oficina del Gobernador del Estado de Zacatecas, Secretaría de Seguridad Pública del Estado de Zacatecas, Secretaría General de Gobierno del Estado de Zacatecas, y PGJE de Zacatecas.

6 MALWARE DE ESTADO



En los últimos años se ha revelado que autoridades mexicanas han adquirido capacidades altamente sofisticadas de vigilancia. En particular, existe evidencia de que distintas autoridades, tanto federales como estatales, **han adquirido la capacidad de infectar computadoras y teléfonos móviles** con distintos tipos de software malicioso, el cual permite a las autoridades extraer información de los dispositivos e incluso tomar control del mismo para convertirlo en un dispositivo completo de vigilancia focalizada.

La utilización de **este método de vigilancia en México es sumamente problemático** por diversas razones. En primer lugar, esta forma de vigilancia otorga un poder invasivo sumamente amplio, el cual difícilmente puede justificarse a la luz de los principios de necesidad y proporcionalidad.[65]

Así mismo, la infección de dispositivos con software de vigilancia ocurre, típicamente, a partir de la explotación de vulnerabilidades en redes, sistemas y dispositivos que, en ocasiones, no son conocidas por el proveedor o fabricante y que ponen en riesgo la privacidad y seguridad de todos los usuarios de esos servicios. Por decir lo menos, esta forma de vigilancia es cuestionable desde el punto de vista ético, sin embargo, dado que la utilización de este método específico de vigilancia no se encuentra regulado de manera específica en alguna ley en México, también es sumamente cuestionable desde el punto de vista legal.

Por otro lado, en virtud de que la utilización de esta técnica de vigilancia normalmente **no requiere la colaboración de empresas de telecomunicaciones**, y que resulta sumamente complicada la detección de dispositivos infectados, existen menos controles y puntos de detección de la utilización abusiva de esta forma de vigilancia. La difícil detección de instancias de vigilancia a través de este método también genera **poderosos incentivos para eludir el control judicial** de las medidas.

Finalmente, la adquisición y operación de estas técnicas sofisticadas de vigilancia representan una erogación de recursos considerable, la cual sucede a partir de procesos de adquisición caracterizados por su opacidad, lo cual abre la puerta para potenciales actos de corrupción.

Por todo lo anterior, la utilización de ataques informáticos para la infección de dispositivos con software malicioso de vigilancia no puede considerarse una ejercicio legítimo del poder del Estado.

En la historia reciente de esta forma de vigilancia, sobresalen las capacidades ofrecidas por tres empresas a autoridades o entidades mexicanas: Hacking Team, NSO Group y FinFisher.

[65] Ver el Capítulo 2 de este informe.

6.1 HACKING TEAM EN MÉXICO

El 5 de julio de 2015, una gran cantidad de correos electrónicos y documentos internos de la firma italiana Hacking Team fueron filtrados al público [66]. 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 Bahréin, Sudán o Uzbekistán.

De un total de 35 naciones, México que resultó ser el principal cliente de la firma [67], con transacciones hechas por parte de diferentes gobiernos locales, dependencias y agencias federales a través de empresas intermediarias y, en prácticamente todos los casos, sin facultades legales para hacerlo. Este gráfico muestra el gasto de México en relación con otros países clientes de Hacking Team.

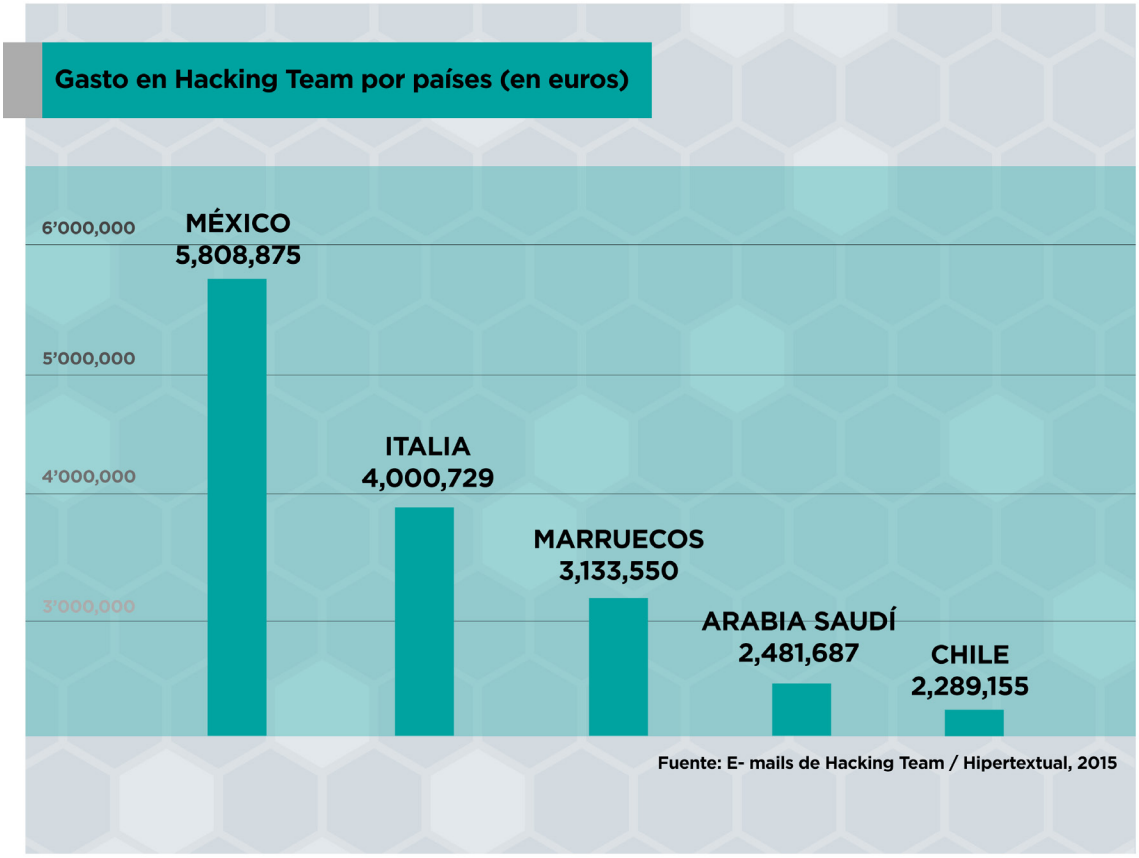


Figura 6.1. Gasto en Hacking Team por países (en euros)

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

[67] 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, el Centro de Investigación y Seguridad Nacional, la Policía Federal, la Procuraduría General de la República y Petróleos Mexicanos. Los siguientes gráficos ilustran qué entidades federativas se encuentran vinculadas con la empresa italiana y cuántos dinero gastaron.

Figura 6.2. Entidades federativas en México con relación comercial con Hacking Team

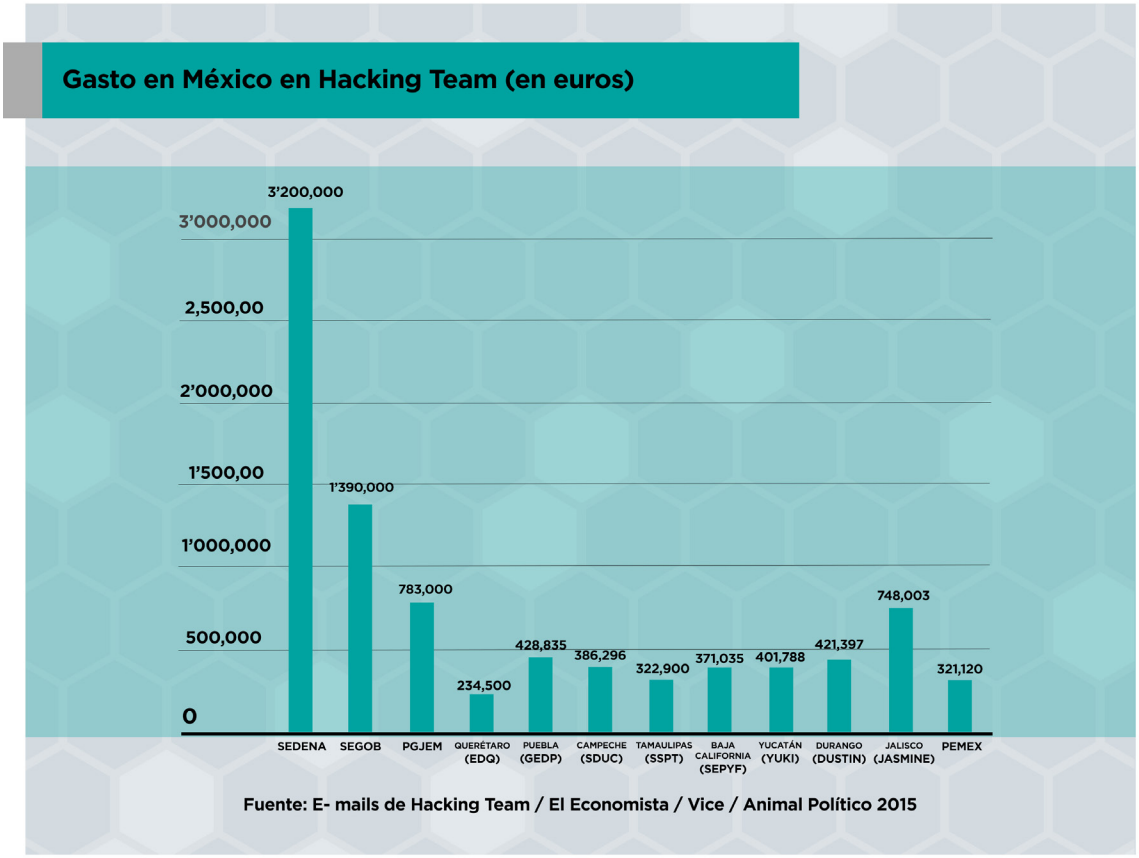


Figura 6.3. Gasto comparativo en México en Hacking Team (en euros)

A pesar de haber negado sus nexos con la firma italiana, estos gobiernos y dependencias suscribieron contratos con empresas intermediarias (Grupo Kabat, SYM Servicios Integrales, DXTX Corp., CloudSec, Neolinx, Grupo Armor, Elite Tactical, TEVA) para adquirir equipo de vigilancia. El siguiente gráfico presenta la relación de estas compañías con sus compradores:

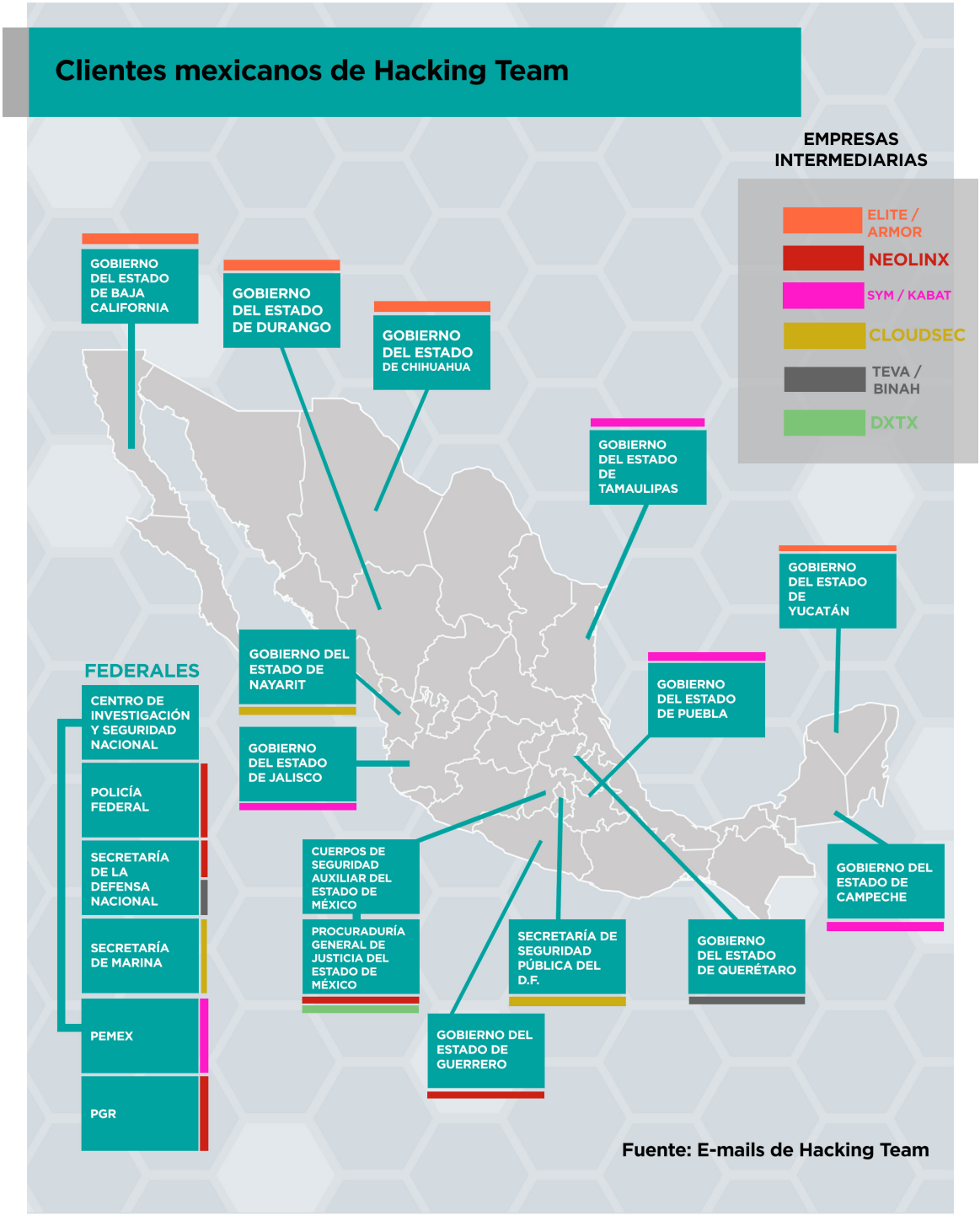


Figura 6.3. Clientes mexicanos de Hacking Team

Uso, abuso y costo de Hacking Team por parte de autoridades mexicanas

Es importante señalar que la gran mayoría de las autoridades que adquirieron el software de Hacking Team no poseen facultades legales o constitucionales para intervenir comunicaciones privadas, **por lo que tanto su adquisición como su uso es claramente ilegal.**

Algunos gobiernos estatales han intentado justificar la adquisición de software de Hacking Team argumentando que sería utilizado por una procuraduría o fiscalía para la investigación de delitos, sin embargo, los datos obtenidos mediante solicitudes de acceso a la información pública levantan serias dudas sobre su uso legal o sobre la justificación de la inversión.

Por ejemplo, Salvador González Reséndiz, Subsecretario de la Secretaría de Planeación, Administración y Finanzas del Gobierno de Jalisco, señaló a la prensa que *"El equipo (de espionaje Galileo) podrá ser usado exclusivamente para secuestro, la Fiscalía avala su buen uso (…)Yo no conozco a esa empresa (Hacking Team) es un tema entre el proveedor y Hacking Team"*. [68]

Sin embargo, además de existir evidencia de que el equipo fue contratado e instalado en una oficina de la Secretaría de Gobierno de Jalisco [69], los datos obtenidos mediante solicitudes de acceso a la información realizadas a la Fiscalía General del Estado de Jalisco y al Consejo de la Judicatura Federal revelan que **dicha Fiscalía únicamente solicitó la autorización judicial para intervenir comunicaciones en dos ocasiones**. Una en el año 2014 y otra en el año 2015.

De lo anterior se desprenden **dos hipótesis**:

1. La Fiscalía General del Estado de Jalisco u otra autoridad perteneciente al gobierno de ese estado han intervenido comunicaciones privadas **utilizando el software de Hacking Team sin autorización judicial**, es decir, de manera ilegal.

2. El Gobierno de Jalisco adquirió software con valor de €748,003.00 euros para utilizarlo en dos ocasiones. Es decir, **cada intervención de comunicaciones privadas habría costado €374,001.5 euros.**

[68] Angel, A. (24 de julio de 2015) El Sabueso: ¿Jalisco compró el sistema de Hacking Team sólo para investigar secuestros? Animal Político. Disponible en: (http://www.animalpolitico.com/elsabueso/el-sabueso-jalisco-compro-galileo-solo-para-investigar-secuestros-y-sin-conocer-a-hacking-team/

[69] Angel, A. (24 de julio de 2015) El Sabueso: ¿Jalisco compró el sistema de Hacking Team sólo para investigar secuestros? Animal Político. Disponible en: http://www.animalpolitico.com/elsabueso/el-sabueso-jalisco-compro-galileo-solo-para-investigar-secuestros-y-sin-conocer-a-hacking-team/

En el caso de las Fiscalías y Procuradurías de Justicia de los Estados de Baja California, Campeche, Durango, Estado de México, Tamaulipas y Yucatán, al responder solicitudes de acceso a la información indicaron no haber solicitado autorización para llevar a cabo la intervención de comunicaciones privadas. El Consejo de la Judicatura Federal tampoco identificó solicitudes provenientes de dichas autoridades. Es decir, **no existe evidencia de que el gasto público erogado por dichas autoridades haya implicado una sola intervención de comunicaciones privadas tramitada de manera legal**, esto a pesar de que el monto asciende a un acumulado de $47,473,269 pesos. [70]

En el caso de los Estados de Puebla, Jalisco y Querétaro, incluso bajo el poco probable supuesto de que el malware de Hacking Team para la intervención de comunicaciones privadas hubiera sido utilizado en todos los casos por 1) autoridades competentes 2) con autorización judicial y 3) en casos en los que era una medida necesaria y proporcional, **el gasto público erogado para ello difícilmente podría ser considerado justificable.**

AUTORIDAD	AÑO DE ADQUISICIÓN [71]	COSTO DE ADQUISICIÓN	SOLICITUDES DE INTERVENCIÓN DE COMUNICACIONES DURANTE EL PERIODO	COSTO[72] POR SOLICITUD DE AUTORIZACIÓN INTERVENCIÓN DE COMUNICACIONES PRIVADAS
Gobierno del Estado de Jalisco	2014	$13,218,409.81	2	$6,609,204.91
Gobierno del Estado de Puebla	2013	$7,578,200.59	8	$947,275.07
Gobierno del Estado de Querétaro	2013	$4,143,990.20	1	$4,143,990.20

[73]

Una radiografía al Remote Control System de Hacking Team

Una de las revelaciones de los correos filtrados de Hacking Team es el sistema de control remoto Galileo (RCS), una plataforma que permite gestionar operaciones de vigilancia. En su explicación más sencilla, 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.

[70] Tipo de Cambio de venta Anual Euro - Peso Mexicano (EUR-MXN) del año 2014 según la Secretaría de Economía. Disponible en: http://portalweb.sgm.gob.mx/economia/es/tipos-de-cambio/eur-mxn.html

[71] Tipo de Cambio de venta Anual Euro - Peso Mexicano (EUR-MXN) del año 2014 según la Secretaría de Economía. Disponible en: http://portalweb.sgm.gob.mx/economia/es/tipos-de-cambio/eur-mxn.html

[72] Tipo de Cambio de venta Anual Euro - Peso Mexicano (EUR-MXN) del año 2014 según la Secretaría de Economía. Disponible en: http://portalweb.sgm.gob.mx/economia/es/tipos-de-cambio/eur-mxn.html

[73] Tabla realizada a partir de los correos electrónicos de Hacking Team y solicitudes de acceso a la información obtenidas por R3D.

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 [74].

El siguiente gráfico ilustra la arquitectura del sistema:

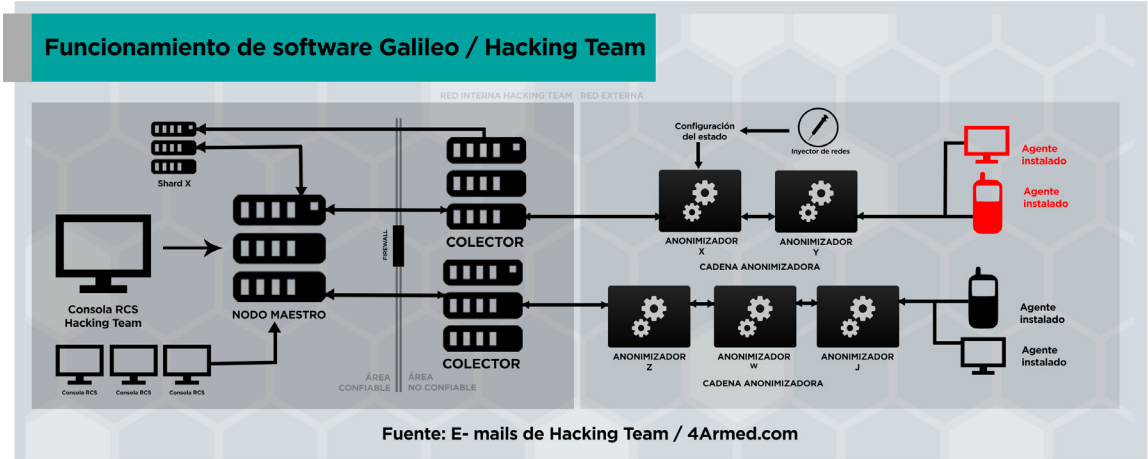


Figura 6.4. Funcionamiento del software Galileo / Hacking Team

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 está 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.

[74] 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

COMPONENTE	FUNCIÓN
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.
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 6.1. Componentes de la arquitectura de Galileo (RCS)

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.

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 celular). 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 solicitaban, 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 vulnerado. Normalmente funcionan una sola vez, por lo que hay una oportunidad de infección.

Una característica importante es el uso de ingeniería social [75] 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 [76]; de forma similar, el gobierno de Querétaro empleó documentos como resoluciones de solicitudes de información para dirigirse a periodistas y sociedad civil [77]. 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". [78]

[75] 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)

[76] Aroche Aguilar, E. (12 de julio de 2015) RMV infectó equipos con archivos exploit para espiar a opositores políticos. Lado B. Disponible en: http://ladobe.com.mx/2015/07/rmv-infecto-equipos-con-archivos-exploit-para-espiar-a-opositores-politicos

[77] 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

[78] Martínez, D. (6 de mayo de 2015) Report SEDENA Mexico. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/6431

Además de los casos mencionados, se detectó el uso de exploits por parte de entidades como Baja California [79], Yucatán [80], Jalisco [81] y el CISEN, que incluso solicitó ayuda para que "los exploits pudieran funcionar dos o tres veces antes de ser borrados." [82]

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, 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 [83], 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 puede 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.

[79] 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

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

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

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

[83] https://wikileaks.org/hackingteam/emails/fileid/511703/237789

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 [84], Chihuahua [85], Guerrero [86], Nayarit [87], Puebla [88], Tamaulipas [89] y Yucatán [90], mientras que en dependencias federales se encuentran la Secretaría de la Defensa Nacional (Sedena) [91], el Centro de Investigación y Seguridad Nacional (CISEN) [92] y Petróleos Mexicanos (Pemex). [93]

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 descargable 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.

Según un *whitepaper* de Hacking Team, la NIA:

> "está diseñada para operar dentro de la red de un proveedor de servicios de Internet (ISP), monitoreando a los suscriptores. En caso de que la conexión de Internet del objetivo esté en un

[84] Scarafile, A. (17 de mayo de 2013) TNI in Stock. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/597097
[85] Velasco, A. (17 de octubre de 2013) Re: HT at ISS Washington 2013. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/4560
[86] Velasco, A. (24 de enero de 2014) Re: PGJ Guerrero in Milan. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/6566
[87] Martínez, D. (20 de marzo de 2015) Report Demo Cyber Police Nayarit Mexico. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/5430
[88] Mokotov, G. (11 de agosto de 2014) RE: COTIZACION HT PUEBLA. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/252042
[89] Bettini, M. (30 de abril de 2014) Re: Prices for Neolinz. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/234499
[90] Scarafile, A. (28 de octubre de 2014) Delivery Mexico (YUKI). E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/16339
[91] Martínez, D. (6 de mayo de 2015) Report SEDENA Mexico. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/6431
[92] Rodriguez-Solís y Guerrero, S. (20 de febrero de 2014) SEGOB Day 1. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/237286
[93] Velasco, A. (19 de diciembre de 2013) Pemex Contract. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/4459

> 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 [94] o Guerrero. [95]

Instalación Remota Móvil: La Instalación Remota Móvil (RMI) es un mecanismo de infección que funciona de la siguiente manera: [96]

> El RMI funciona mandando 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.

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 ha documentado el uso de este método de infección en estados como Querétaro [97], Guerrero [98], Jalisco [99] y Puebla [100], así como la Sedena, que incluso preguntó a los técnicos de Hacking Team si había forma de modificar la cabeza de un mensaje. [101]

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

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

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

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

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

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

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

[101] Martínez, D. (6 de mayo de 2015) Report SEDENA Mexico. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/6431

6.2 NSO GROUP EN MÉXICO

En agosto de 2016, Citizen Lab [102], un laboratorio interdisciplinario de la escuela Munk de Asuntos Globales de la Universidad de Toronto, Canadá, reveló información sobre un sofisticado software de vigilancia comercializado a gobiernos por la empresa NSO Group, denominado *Pegasus*.

Según documenta Citizen Lab, el 10 y 11 de agosto de 2016, **Ahmed Mansoor,** defensor de derechos humanos en los Emiratos Árabes Unidos (EAU), recibió mensajes de texto (SMS) en su iPhone [103]. Estos mensajes **supuestamente contenían "secretos" sobre los detenidos torturados** en las cárceles de EAU. Dicha información podía ser consultada al hacer **clic en un enlace.**

En lugar de acceder al enlace, Ahmed Mansoor envió los mensajes de texto a Citizen Lab para su análisis.

Los investigadores de Citizen Lab pudieron verificar que los enlaces estaban ligados a la infraestructura de NSO Group, una empresa israelí de software que comercializa *Pegasus*, un spyware de "intercepción legal" que, según dicha empresa, únicamente se comercializa para el uso de gobiernos. [104]

¿Cómo se relaciona un SMS a NSO Group?

Uno de los enlaces enviado vía SMS a Mansoor redirigía hacia el dominio **webadv.co**, el cual ya había sido identificado anteriormente por el Citizen Lab como parte de la red de *exploits* de NSO Group. El equipo de investigadores encontró dicha infraestructura gracias a una investigación previa en mayo de 2016 [105] *(Stealth Falcon)*, y consta de al menos 237 direcciones IP activas.

Para comprobar la hipótesis de que los enlaces contenidos en los mensajes recibidos por Mansoor podrían resultar en la infección del dispositivo, **los investigadores del Citizen Lab utilizaron un iPhone 5 nuevo** con la misma versión de sistema operativo que el

[102] Citizen Lab (2016) About Citizen Lab. Disponible en: https://citizenlab.org/about/

[103] Marczak, B. y J. Scott-Railton (24 de agosto de 2016) The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender. The Citizen Lab. Disponible en: https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

[104] NSO Group (s/f) NSO Group. Disponible en: https://web.archive.org/web/20120813064018/http://www.sibat.mod.gov.il/NR/rdonlyres/DADE8D1E-DFAA-4143-BB48-A73C77C88CBA/0/NSOGROUPE.pdf

[105] Marczak, B. y J. Scott-Railton (29 de mayo de 2016) Keep Calm and (Don't) Enable Macros: A New Threat Actor Targets UAE Dissidents. The Citizen Lab. Disponible en: https://citizenlab.org/2016/05/stealth-falcon/

celular de Mansoor (iOS 9.3.3). Ingesaron manualmente la dirección URL proporcionada a Mansoor en el mensaje de texto (SMS) en el navegador Safari. Al acceder al enlace, apareció una página en blanco y, posteriormente, el navegador se cerró. Sin embargo, descubrieron que un software desconocido fue implantado en el dispositivo como producto de ese acceso Web.

Citizen Lab pudo identificar que el software aprovechaba una vulnerabilidad de seguridad inédita [106] *(zero-day exploit)* en iOS, bautizada como *Trident* [107]. A través de esta infección, se hacía un *jailbreak* [108] al dispositivo y se instalaba un sofisticado spyware que habría permitido al atacante tomar control de diferentes funciones y acceder a los contenidos del aparato. Entre los permisos adquiridos, se encuentran:

- Acceso a la información guardada en el dispositivo como: archivos, datos del calendario, listas de contactos, contraseñas, entre otros.
- Acceso a mensajes de texto, así como datos de otras aplicaciones como Gmail, WhatsApp, Skype, Facebook, Telegram.
- Acceso a escuchar llamadas realizadas por teléfono, a través de WhatsApp o Viber.
- Permisos para grabar activa o pasivamente utilizando el micrófono y la cámara del dispositivo.

[106] Colaboradores de Wikipedia (2016) Ataque de día cero. Disponible en: https://es.wikipedia.org/wiki/Ataque_de_d%C3%ADa_cero

[107] Brotherson, L. (30 de agosto de 2016) iPhone Spyware Trident Exploit Chain. Leviathan Security Group. Disponible en: http://www.leviathansecurity.com/blog/iphone-spyware-trident-exploit-chain

[108] El jailbreak es una práctica de desbloqueo de candados digitales que permite a un usuario tener acceso completo al sistema operativo, obteniendo mayores privilegios para realizar acciones como descargar aplicaciones, instalar programas y/o utilizar funciones del dispositivo que suelen ser limitadas por los desarrolladores. Colaboradores de Wikipedia (2016) Jailbreak (iOS). Disponible en: https://es.wikipedia.org/wiki/Jailbreak_(iOS).

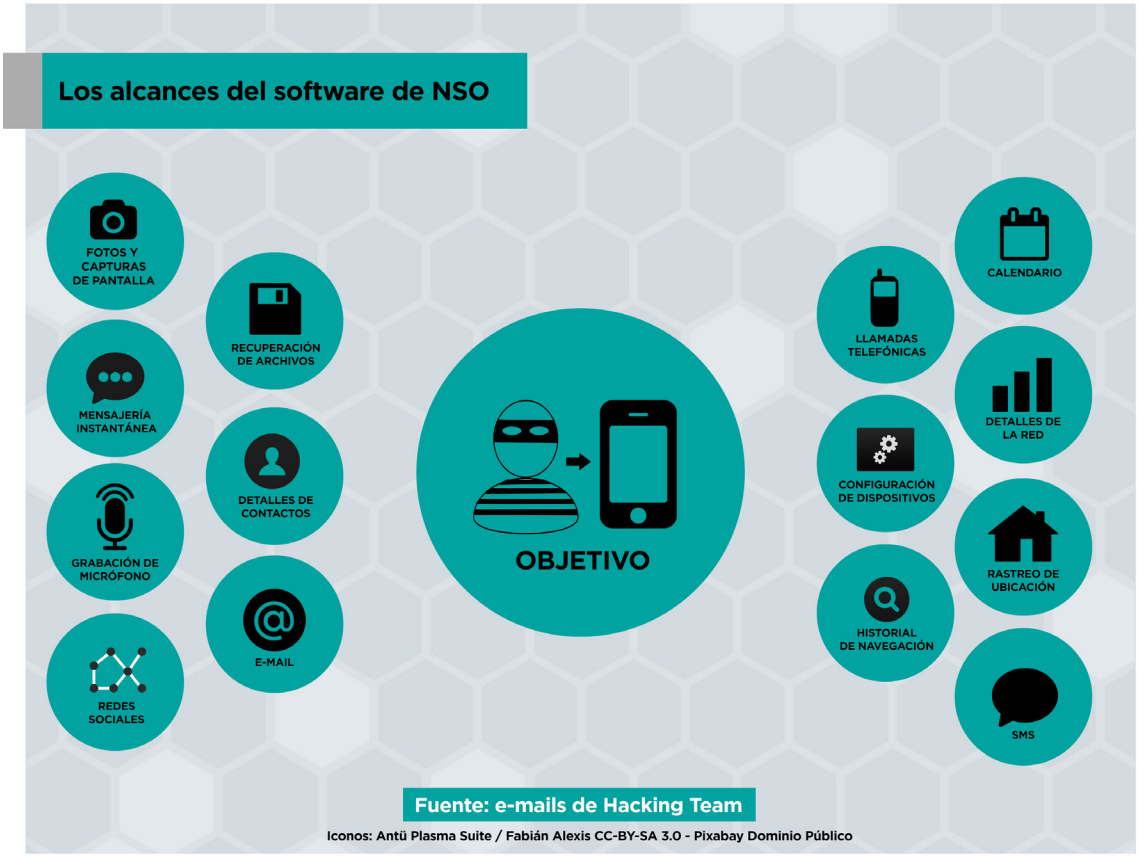


Figura 6.5. Alcances del software Pegasus de NSO Group

¿Por qué alguien daría clic a SMS anónimos?

Para obtener el clic que permite la infección del dispositivo, **el atacante debe asegurarse de engañar al objetivo**. Para ello, se envían mensajes diseñados para aparentar ser legítimos. En este punto, cobra especial relevancia la infraestructura de NSO Group, ya que los dominios que pertenecen a esta buscan suplantar a otros sitios legítimos como medios de comunicación, servicios de telecomunicaciones, redes sociales, portales de gobierno, organizaciones humanitarias, aerolíneas, entre otros.

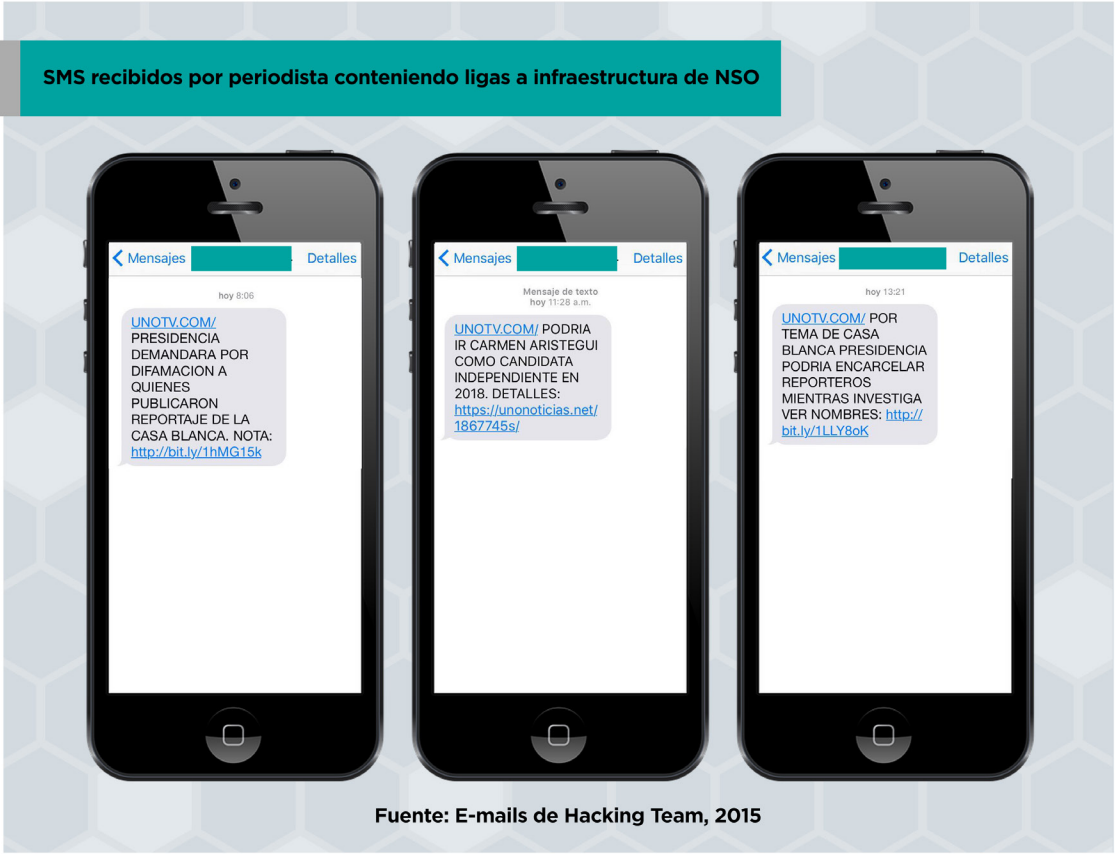


Figura 6.6. SMS recibidos por periodista mexicano con enlaces a infraestructura de NSO Group

Según la investigación de Citizen Lab, la mayoría de los dominios de la infraestructura de NSO se encuentran vinculados a México, lo cual hace presumir que autoridades mexicanas son clientes de NSO [109] y que personas en México podrían haber sido objetivos de esta forma de vigilancia.

[109] Esta presunción, además, se encuentra soportada por las menciones constantes a NSO Group como proveedor de equipo de vigilancia en distintos correos de la filtración de Hacking Team.

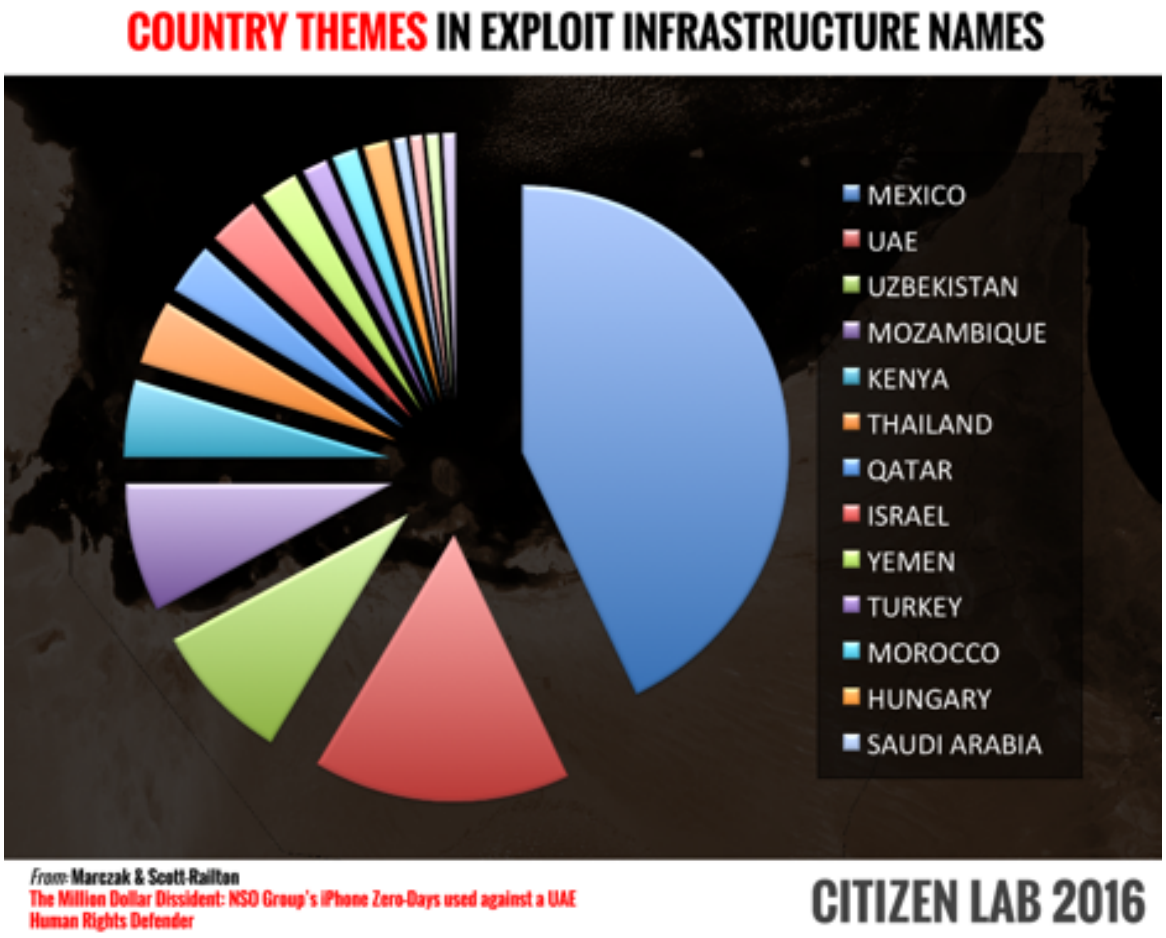


Figura 6.7. Países por representación en la infraestructura de exploits de NSO Group

Entre los dominios con algún vínculo a sitios web en México se encontraron, entre otros:

- Unonoticias.net
- Univision.click
- Iusacell-movil.com.mx
- Y0utube.com.mx
- Fb-accounts.com
- Googleplay-store.com
- Whatsapp-app.com

Como se puede observar de los mensajes recibidos por un periodista mexicano y la lista de los sitios web parte de la infraestructura de NSO, **estos son diseñados de tal modo que puedan parecer legítimos a primera vista y normalmente explotan un sentido de**

urgencia o necesidad propia del objetivo, esto se llama "ingeniería social" y es parte del proceso de NSO para lograr el clic necesario como vector de infección.

¿Qué sucede una vez que la persona objetivo hace clic en un SMS de NSO?

Una vez que el objetivo hace clic en el enlace, el sitio web empleado para la infección (denominado *Anonymizer*) envía una solicitud al servidor de instalación del spyware (*Pegasus Installation Server*) ubicado en las instalaciones de quien opera el ataque. Este servidor examina si el dispositivo a infectar tiene una vulnerabilidad que el spyware pueda explotar, como la del *Trident* en iOS. Existen dos escenarios posibles:

- Si el dispositivo posee una vulnerabilidad, el servidor envía el exploit adecuado a través del sitio web *(Anonymizer)* para intentar una infección.
- Si la infección falla por cualquier motivo, el navegador del objetivo será redirigido a un sitio web legítimo determinado previamente por el atacante, con la finalidad de evitar suspicacias.

Además de obtener los permisos previamente descritos, el spyware envía la información recolectada al *Pegasus Data Server* a través de la *Pegasus Anonymizing Transmission Network*, un sistema de proxies en cadena. Eso permite que el atacante pueda visualizar y procesar la información obtenida en una estación de trabajo *(Pegasus Working Station)*. La siguiente gráfica ilustra el funcionamiento general del sistema:

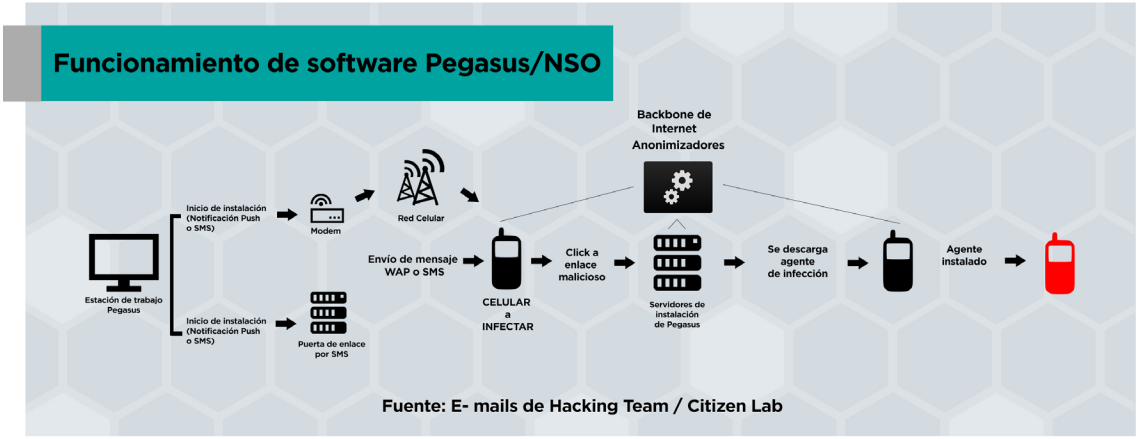


Figura 6.8. Funcionamiento del software Pegasus de NSO Group

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.

Una vez que se dio a conocer el caso, **Apple liberó un parche de seguridad para Mac OS X y Desktop Safari el 1 de septiembre de 2016**, así como para iOS con la versión 9.3.5 de su sistema operativo [110]. Sin embargo, el Citizen Lab menciona que "las vulnerabilidades usadas por NSO pudieron haber sido usadas contra usuarios de dispositivos sin iOS, incluyendo OSX". o inclusive otros dispositivos y sistemas operativos.

El reporte de Citizen Lab también concluye que el costo por infección mediante el sistema Pegasus es sumamente elevado, ya que los exploits para el sistema operativo de Apple son raros y costosos. Con base en ello, los investigadores apuntan que, en el caso de Mansoor, el gobierno de los Emiratos Árabes Unidos era el sospechoso más probable detrás del ataque.

LOS POSIBLES CLIENTES DE NSO EN MÉXICO

Existe evidencia de que agencias del gobierno mexicano han adquirido el spyware de NSO Group. Diversa información apunta a que posiblemente SEDENA, PGR y CISEN habrían comprado el software de NSO.

NSO en los correos de Hacking Team

De acuerdo con los correos filtrados de Hacking Team, el ingeniero Sergio Rodríguez-Solís reportó que, en una visita hecha al CISEN el 15 de enero de 2014 [111], "ellos explicaron que había probado por sí mismos un sistema de infección 'manos libres' para teléfonos móviles que funcionaba en hasta 80% de los dispositivos que probaron, incluyendo Android, BB, iOS y Symbian. Se quejaron de por qué nosotros no tenemos vectores de infección que no requieren de la interacción del usuario como NSO tiene."

En la misma comunicación, Rodríguez-Solís relata un encuentro con la SEDENA, en el que indica que "está dividida en cuatro grupos". El ingeniero menciona que todos los equipos están en conflicto y que "tienen NSO para móviles y están 'enamorados' de ello". Igual apunta que el precio de venta de NSO comienza en 18 millones, por lo que "deben ser muy cuidadosos en explicar por qué tanta diferencia" respecto a los precios de Hacking Team.

Días después, el 29 de enero de 2014, Alex Velasco, vendedor de Hacking Team, mencionó en un correo a su equipo que la SEDENA estaba buscando un contrato con 600 agentes [112]. "Ellos también compraron NSO hace dos años y actualmente no está funcionando. Fueron engañados por el revendedor de NSO y quieren estar seguros que nosotros no somos solo otra mentira."

[110] Apple Security Updates (2016) Disponible en: https://support.apple.com/en-us/HT201222

[111] Rodríguez Solís, S. (19 de enero de 2014) México Jan 2014. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/5275

[112] Velasco, A. (29 de enero de 2014) SEDENA visit to HT HQ. E-mail. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/8964

Así mismo, el 28 de noviembre de 2014, Armando Pérez, integrante de la firma Grupo Tech Bull S.A. de C.V., envió un correo a la dirección info@hackingteam.com [113]. En el mensaje, Pérez explica que Grupo Tech Bull es "una compañía que vende inteligencia y seguridad al gobierno mexicano." Describe a la empresa como una subsidiaria de una compañía principal (Balam Seguridad), y enlista a la Marina, la PGR, el CISEN, la Policía Federal y "un montón" de Procuradurías, incluyendo la del Estado de México. Líneas delante, Pérez menciona contratos con NSO Group:

> "Nosotros [Grupo Tech Bull] apenas vendimos a la **PGR** (con contrato ya firmado y ellos ya enviaron el dinero) el sistema **NSO Pegasus**. Teníamos un acuerdo con ellos con respecto al precio por 500 infecciones. Cuando ellos [NSO Group] se percataron que habíamos firmado el contrato, se volvieron locos e incrementaron el precio en 50%, por lo que decidimos cancelar el trato con ellos."
>
> "El problema aquí es que Tomás Zerón, quien está a cargo de esta nueva área en la PGR [Agencia de Investigación Criminal], solía trabajar en la PGJ del Estado de México (él les compró el sistema a ustedes) y sigue diciéndole a todos que el sistema que instalaron en Toluca no funciona y que él no lo quiere en la PGR. Nuestro trabajo es convencerlo de que su sistema trabaja de forma similar. Sabemos en definitiva que **NSO es mejor porque algunas de sus infecciones son invisibles, tiene mejores capacidades y ha trabajado realmente bien y con resultados probados en México (SEDENA y CISEN).**

El 29 de noviembre de 2014, Marco Bettini, representante de ventas de Hacking Team, le respondió a Armando Pérez, integrante de la firma Grupo Tech Bull S.A. de C.V., pidiéndole la propuesta técnica de NSO Group "para proveer una oferta competitiva directa y convencer al cliente de nuestras capacidades de solución". El 1 de diciembre, Pérez respondió el correo a Bettini, **adjuntando la presentación de NSO** y solicitando al representante de Hacking Team que "destaque las ventajas de su sistema sobre el de NSO."

Contratos con SEDENA

Un reportaje del portal *Contralínea*, publicado el 22 de julio de 2012 y firmado por Zósimo Camacho [114], señala que ocho contratos celebrados entre la Secretaría de la Defensa Nacional (SEDENA) y la empresa Security Tracking S.A. de C.V. estaban bajo

[113] Pérez, A. (1 de diciembre de 2014) Re: QUOTE MEXICO URGENT. E-mail. Disponible en: https://wikileaks.org/hacking-team/emails/emailid/5391

[114] Camacho, Z. (22 de julio de 2012) Sedena, bajo escrutinio por ocho contratos de 5.6 mil MDP. Contralínea. Disponible en: http://www.contralinea.com.mx/archivo-revista/index.php/2012/07/22/sedena-bajo-escrutinio-por-ocho-contratos-de-5-6-mil-mdp/

investigación por parte de la Secretaría de la Función Pública, la Auditoría Superior de la Federación y la Inspección y Contraloría General del Ejército y Fuerza Aérea.

De acuerdo con el reportaje, "el objetivo de los ocho contratos fiscalizados fue incrementar las capacidades de espionaje y procesamiento de información de inteligencia de la Sedena". Según las fuentes citadas, "el Ejército Mexicano y la Fuerza Aérea Mexicana construyeron un Sistema de Inteligencia Regional para modernizar el Centro de Comando y Control, sus subcentros y módulos, y **construir la Plataforma Pegasus."**

Tres contratos sobre la adquisición del sistema Pegasus por parte de la SEDENA fueron publicados el 16 de julio de 2012 por el portal *Aristegui Noticias*.[115] [116] [117]

Cabe señalar que la **SEDENA no posee facultades legales para la intervención de comunicaciones privadas**, por lo que su adquisición y uso, en cualquier caso, sería indudablemente ilegal.

Contratos con PGR

El 12 de Septiembre de 2016, el periódico *Reforma* publicó una nota periodística titulada "Adquiere PGR equipo para espiar" [118]. En ella se identifica a la PGR como la adquirente del software de NSO por 15 millones de dólares:

> "La semana pasada, *The New York Times* informó que el Gobierno de México pagó 15 millones de dólares por este sistema de intercepción desarrollado por la empresa israelí NSO Group, aunque no precisó la institución responsable de adquirirlo. Sin embargo, autoridades de la Administración federal informaron que la PGR de Murillo fue la que contrató el software y que no fue una sola compra, sino dos: en 2014 y el año pasado. Indicaron que la segunda entrega se hizo poco después de que Arely Gómez asumiera el cargo, aunque el contrato ya estaba finiquitado desde antes de la salida de Murillo."

[115] Los 5 contratos de Sedena para espiar celulares y comunicación por internet (16 de julio de 2012) Aristegui Noticias. Disponible en: http://aristeguinoticias.com/1607/mexico/a-detalle-los-5-contratos-de-sedena-para-espionaje-de-celulares-y-radios/

[116] Contrato disponible en: https://www.scribd.com/document/100213906/Gobierno-federal-via-Sedena-compro-5-mil-mdp-en-equipo-para-espionaje-27-de-julio-2011

[117] Contrato disponible en: https://www.scribd.com/document/100223409/Gobierno-federal-via-Sedena-compro-5-mil-mdp-en-equipo-para-espionaje-29-de-marzo-2012

[118] Adquiere la PGR equipo para espiar (12 de septiembre de 2016) Reforma. Disponible en: http://www.reforma.com/aplicacioneslibre/preacceso/articulo/default.aspx?id=937450

Esta información coincide con correos filtrados de la empresa Hacking Team en los que se hace referencia a una supuesta puja entre las empresas NSO y Hacking Team. Inclusive se hacen suposiciones de supuesta corrupción en la adquisición del equipo de NSO. En un correo de 26 de agosto de 2014 [119], un empleado de Hacking Team escribe lo siguiente:

> "Hola,
>
> Acabo de hablar con Gilberto [120] y me dijo que se está enfrentando a una gran oposición por parte de Ori que está empujando a NSO. Ori se ha hecho buen amigo del hijo del jefe de adquisiciones (procurement chief) y está ofreciendo NSO por 15 millones de dólares. Estoy seguro que hay algunos buenos sobornos sucediendo con esta compra."

[119] https://wikileaks.org/hackingteam/emails/emailid/6584

[120] Refiere a Gilberto Enríquez, de la empresa Neolinx, vinculado con la venta de equipos de vigilancia de Hacking Team a Guerrero, Estado de México y al CISEN.

7 CONCLUSIÓN: FUERA DE CONTROL

Durante años en México se ha propagado el discurso que exige a la ciudadanía aceptar la erosión de sus derechos ofreciendo, a cambio, la garantía de su seguridad. A la luz de la evidencia la seguridad está muy lejos de ser garantizada, sin embargo, la vigencia práctica de los derechos si se encuentra en retroceso. Este contexto se agrava al reconocer que México atraviesa una crisis de derechos humanos en donde no es poco común encontrar que el propio Estado que ha ofrecido seguridad ha sido el perpetrador de graves violaciones.

Como ha quedado documentado en este informe, el caso de la vigilancia no ha escapado a este discurso. **Se ha promovido la expansión de las facultades legales para llevar a cabo medidas de vigilancia sin que al mismo tiempo se hayan impuesto controles democráticos a las mismas.** El marco legal se ha diseñado deficientemente, a veces de manera deliberada, para dar pie a interpretaciones que permitan a más autoridades vigilar sin contrapesos institucionales que pongan en riesgo la garantía de impunidad.

Podemos afirmar que los esfuerzos de la sociedad civil han permitido hacer resistencia al avance de la lógica de la vigilancia sin controles. A través de distintos recursos, se han logrado establecer **obligaciones de transparencia** que nos permitirán conocer y evaluar mejor el alcance y volumen de la vigilancia en el país; el litigio estratégico y la incidencia han permitido que **hoy todas las medidas de vigilancia requieran de control judicial y las autoridades facultadas para ejercer vigilancia estén delimitadas** claramente por el poder judicial. No obstante, también se han institucionalizado métodos abusivos y desproporcionados de vigilancia como la conservación masiva e indiscriminada de datos de usuarios de telecomunicaciones, la cual R3D combate ahora ante organismos internacionales de derechos humanos.

Pero a la dimensión legal se le opone la realidad concreta. La investigación sobre la práctica de la vigilancia en México arroja conclusiones sumamente preocupantes. En este informe se ha documentado que **la gran mayoría de las medidas de vigilancia se ha llevado a cabo sin control judicial.** También que un número importante de autoridades han ejercido la vigilancia, e incluso han adquirido millonarias capacidades tecnológicas altamente invasivas, **sin siquiera tener facultades legales** para la intervención de comunicaciones privadas.

Se ha documentado también que la **utilización de medidas de vigilancia por autoridades de procuración de justicia no ha tenido como resultado ejercicios de acción penal**, sino que la gran mayoría de los casos se han vigilado personas que jamás son llevadas a juicio por la probable comisión de un delito.

Se ha evidenciado también que **las obligaciones de transparencia no se han cumplido en la práctica** y que incluso utilizando los mecanismos institucionales para conocer información pública sobre el ejercicio de la vigilancia estatal, **persiste gran resistencia de parte de las autoridades a entregar información,** esto a pesar de que los órganos garantes han determinado su publicidad. Peor aún: en los casos que se ha logrado el acceso, la información revelada por autoridades, jueces y empresas es en ocasiones contradictoria o incompleta.

La vigilancia en México está fuera de control.

NOV 2016

R3D

Red en Defensa
de los Derechos Digitales