PRIVACY INTERNATIONAL

Informe de actor interesado
Examen Periódico Universal
31o periodo de sesiones - México

El Derecho a la Privacidad en los Estados Unidos Mexicanos

Presentado por la Red en Defensa de los Derechos Digitales (R3D) y Privacy International

Marzo 2018

Informe de actor interesado Examen Periódico Universal 31o periodo de sesiones - México

Marzo 2018

PRIVACY INTERNATIONAL

www.privacyinternational.org

R3D
Red en Defensa de los Derechos Digitales

INTRODUCCIÓN

1. Este informe es presentado por la Red en Defensa de los Derechos Digitales (R3D) y Privacy International (PI). La Red en Defensa de los Derechos Digitales (R3D) es una organización no gubernamental, sin fines de lucro, ubicada en México, dedicada a la defensa de los derechos humanos en el entorno digital. Privacy International (PI) es una organización no gubernamental sin fines de lucro ubicada en Londres enfocada en la defensa, promoción y protección del derecho a la privacidad alrededor del mundo.

2. PI y R3D desean presentar preocupaciones en torno a la situación de violación al derecho a la privacidad en México, para su consideración en el próximo examen a México dentro de la sesión 31 del Grupo de Trabajo del Examen Periódico Universal (EPU).

Derecho a la Privacidad

3. La privacidad es un derecho fundamental reconocido en numerosos instrumentos internacionales de derechos humanos.[1] El derecho a la privacidad posibilita el ejercicio de otros derechos como el derecho a la libertad de expresión, libre asociación, el acceso a la información y es esencial para la dignidad de las personas y la viabilidad de los sistemas democráticos.

4. Las afectaciones al derecho a la privacidad sólo pueden ser justificadas cuando son establecidas por ley, necesarias para lograr un fin legítimo y proporcionales al objetivo perseguido.

5. A partir del desarrollo de tecnologías de la información que han posibilitado la recopilación, conservación y el tratamiento masivo de datos, la protección al derecho a la privacidad se ha expandido al tratamiento de datos personales. Varios instrumentos internacionales incluyen principios de protección de datos personales[2] y se ha incorporado en muchas leyes nacionales, como en la mexicana, tales principios.[3]

[1] Declaración Universal de Derechos Humanos Artículo 12, Convención de las Naciones Unidas sobre Trabajadores Migrantes Artículo 14, Convención de Naciones Unidas sobre los Derechos del Niño Artículo 16, Pacto Internacional sobre Derechos Civiles y Políticos Artículo 17; convenciones regionales incluyendo artículo 10 de la Carta Africana sobre los Derechos y el Bienestar del Niño, Artículo 11 de la Convención Americana sobre Derechos Humanos, Artículo 4 de los Principios de la Unión Africana sobre Libertad de Expresión, Artículo de la Declaración Americana de los Derechos y Deberes del Hombre, Artículo 21 de la Carta Árabe sobre Derechos Humanos y Artículo 8 de la Convención Europea para la Protección de los Derechos Humanos y las Libertades Fundamentales; Principios de Johannesburgo sobre Seguridad Nacional, Libertad de Expresión y Acceso a la Información, Principios de Camden sobre Libertad de Expresión e igualdad.

[2] Consultar: Consejo de la Convención Europea para la Protección de Individuos con respecto al Procesamiento Automático de Datos Personales (Nº 108), 1981; Guía sobre protección de la privacidad y flujo transfronterizo de datos personales de la Organización para la Cooperación y el Desarrollo Económico (1980) y la Guía para la regulación de bases de datos personalizadas (Resolución 45/95 de la Asamblea General y E/CN.4/1990/72).

[3] Al 25 de enero de 2018, más de 100 países alrededor del mundo han adoptado leyes integrales de protección de datos personales y aproximadamente cuarenta países tienen pendiente la aprobación de leyes o iniciativas dedicadas a la protección de datos personales. Banisar, David, National Comprehensive Data Protection/Privacy Laws and Bills 2018. 25 de enero de 2018. Disponible en: https://ssrn.com/abstract=1951416

El derecho a la privacidad en México

6. La Constitución Política de los Estados Unidos Mexicanos reconoce el derecho a la privacidad en el artículo 16, que determina:

"Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento".[4]

7. Respecto del derecho a la privacidad de las comunicaciones privadas, el artículo 16 constitucional también señala que:

"Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley.

Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de la misma y su duración. La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor."

8. La Ley Federal de Protección de Datos Personales en Posesión de los Sujetos Obligados[5] y la Ley Federal de Protección de Datos Personales en Posesión de Particulares[6] regulan el tratamiento de datos personales en México.

9. La Constitución de México considera que todas las normas de derechos humanos contempladas en tratados internacionales se encuentran en el mismo nivel jerárquico que la Constitución. México es parte de todos los principales tratados de derechos humanos del sistema universal y del sistema interamericano de derechos humanos.

Seguimiento del EPU anterior

10. El reporte presentado por México durante la sesión 17va del Examen Periódico Universal, que tomó lugar en octubre de 2013, no menciona el derecho a la privacidad. En los exámenes realizados a México en las sesiones pasadas

[4] Constitución Política de los Estados Unidos Mexicanos Artículo 16. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/1_150917.pdf

[5] Disponible en http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

[6] http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

tampoco han habido recomendaciones por parte de los demás Estados miembros sobre el derecho a la privacidad, aun cuando habían varias recomendaciones sobre la necesidad de adoptar medidas apropiadas para proteger a periodistas y defensores de derechos humanos.

11. El resumen de los reportes presentados por varios interlocutores durante el examen anterior realizado a México incluye una recomendación presentada por Privacy International (PI) sobre la necesidad de contar con regulación y supervisión estricta por parte de autoridades judiciales y otras autoridades independientes sobre el uso de programas informáticos de vigilancia.[7]

ÁREAS DE PREOCUPACIÓN

A. La inadecuada regulación de la vigilancia de comunicaciones en México

12. En los últimos años, el Estado Mexicano ha incrementado sus facultades legales y su capacidad técnica para implementar medidas de vigilancia. Por ejemplo, se han expedido y reformado leyes como la Ley Federal de Telecomunicaciones y Radiodifusión, el Código Nacional de Procedimientos Penales y otras leyes para establecer medidas de vigilancia como las siguientes:

1. Retención masiva e indiscriminada de datos de comunicaciones

13. El artículo 190, fracción II, de la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR) obliga a las empresas de telecomunicaciones a conservar, por dos años, un registro de comunicaciones de todos sus usuarios de manera indiscriminada. Este registro incluye una serie de datos conocidos como "metadatos de comunicaciones" como lo son: el origen y destino de las comunicaciones; su fecha, hora y duración; datos de identificación de los comunicantes y los dispositivos; e incluso la localización geográfica de los usuarios.

14. La revelación o análisis de estos datos puede comprometer la privacidad de todos los usuarios. La generación de este registro masivo e indiscriminado compromete de manera severa la privacidad, especialmente en caso de acceso ilícito a los mismos, producto de ataques informáticos o actos de corrupción.

15. Es por ello que, por ejemplo, el Tribunal de Justicia de la Unión Europea ha invalidado disposiciones legales que contemplan obligaciones de conservación masiva e indiscriminada, en tanto no resultan restricciones necesarias o proporcionales al derecho a la privacidad[8], el Consejo

[7] Resumen preparado por la Oficina del Alto Comisionado para los Derechos Humanos con arreglo al párrafo 15 b) del anexo de la resolución 5/1 del Consejo de Derechos Humanos y al párrafo 5 del anexo de la resolución 16/21 del Consejo. Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/160/17/PDF/G1316017.pdf?OpenElement

[8] TJUE. Digital Rights Ireland vs. Minister of Communications, Marine and Natural Resources y otros. Casos Conjuntos, C-293/12 y C-594/12, 8 de abril de 2014. Disponible en: http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0293&lang1=es&type=TXT&ancre=. Ver también TJUE. Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson y otros. Casos conjuntos C-203/15 y C-698/15, 21 de diciembre de 2016. Disponible en: http://curia.europa.eu/juris/celex.jsf?celex=62015CJ0203&lang1=en&type=TXT&ancre=

de Derechos Humanos de Naciones Unidas ha reconocido que los "metadatos, cuando son agregados, pueden revelar información personal que es tan sensible como el contenido de las comunicaciones",[9] y el Comité de Derechos Humanos ha declarado en el mismo sentido que las políticas de retención de datos constituyen una interferencia con el derecho a la privacidad y que como regla general los Estados deben "abstenerse de imponer esquemas de retención de datos por terceras partes".[10]

2. El acceso a datos de comunicaciones y la geolocalización en tiempo real

16. Tanto el acceso a los datos conservados por las empresas de telecomunicaciones, como el monitoreo, en tiempo real, de la localización de las y los usuarios de telecomunicaciones se encuentra regulada de manera deficiente en México. Por ejemplo, la LFTR no establece de manera clara, precisa y detallada qué autoridades pueden llevar a cabo dichas medidas de vigilancia, ni establecen las circunstancias y los procedimientos.

17. Tampoco se establece, de manera explícita, la necesidad de autorización judicial para llevar a cabo estas medidas de invasión a la privacidad. Lo anterior, tomando en cuenta el contexto de violaciones a los derechos humanos en México donde, además, el crimen organizado opera con la tolerancia, aquiescencia, control o dirección de parte de funcionarios públicos, el riesgo a la privacidad, la seguridad, la integridad física y la vida de la población se encuentra gravemente comprometida por medidas de vigilancia sin salvaguardas contra el abuso.

3. La ausencia de salvaguardas adecuadas contra la vigilancia abusiva

18. La legislación mexicana no contempla salvaguardas adecuadas y suficientes en contra del abuso de medidas de vigilancia secreta. Además de no establecerse de manera clara y explícita la necesidad de control judicial previo para todas las medidas de vigilancia, la legislación no contempla medidas como la supervisión independiente o el derecho de notificación al afectado. Lo anterior impide la detección, investigación y sanción de ejercicios abusivos de vigilancia.

19. Asimismo, si bien la legislación en materia de transparencia contempla algunas obligaciones de transparencia proactiva relativas a medidas de vigilancia, como publicar estadísticas sobre el empleo de vigilancia, en la práctica éstas no han sido implementadas y, de manera rutinaria, las autoridades y el poder judicial niegan el acceso a las mismas, incluso a versiones redactadas, lo cual impide el control social de estas actividades.

[9] Resolución del Consejo de Derechos Humanos sobre el derecho a la privacidad en la era digital, UN doc. A/HRC/RES/34/7.

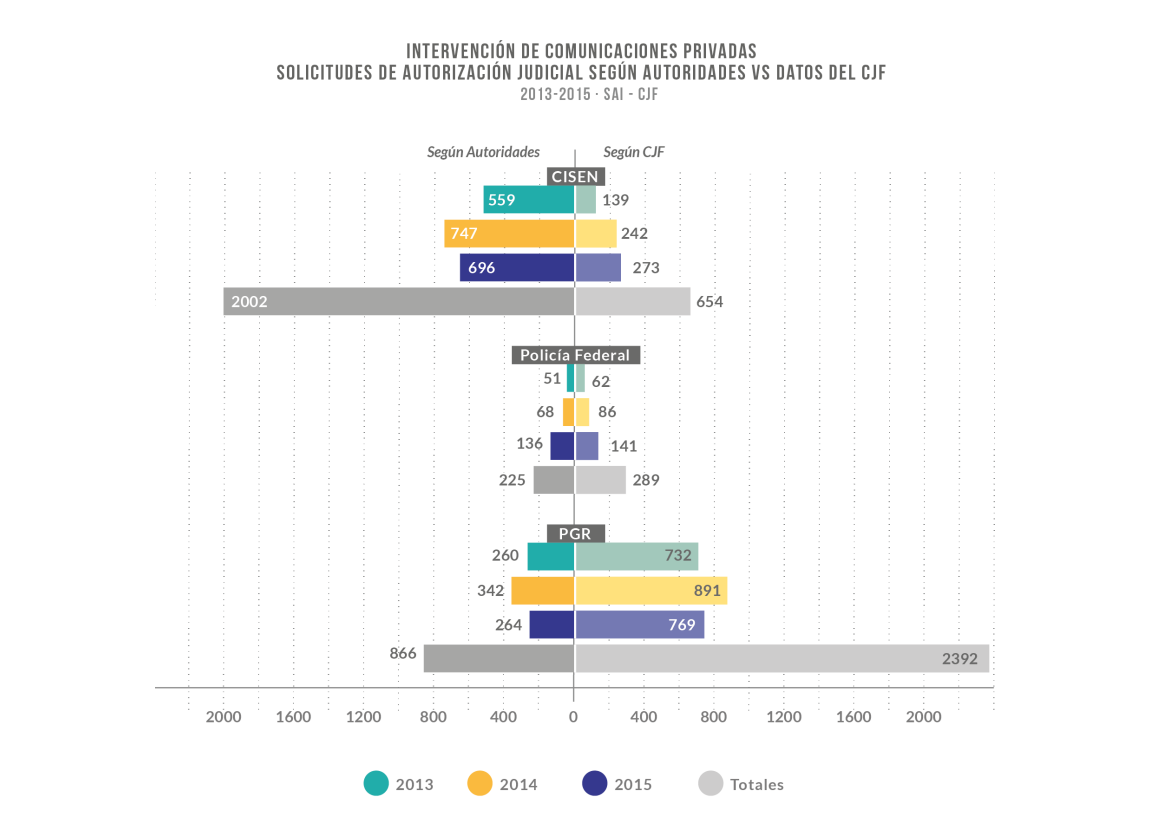
[10] Observaciones finales del cuarto reporte periódico de los Estados Unidos de América. Comité de Derechos Humanos de la ONU, U.N. Doc. CCPR/C/USA/CO/4, para. 22 (23 April 2014).

B. La vigilancia ilegal y sin controles en México

20. Además de las deficiencias en la regulación de la vigilancia en México, se ha documentado el ejercicio ilegal y sin control de la vigilancia en México. En el Informe *"El Estado de la Vigilancia: Fuera de Control"*,[11] la Red en Defensa de los Derechos Digitales (R3D) documenta diversas inconsistencias e ilegalidades.

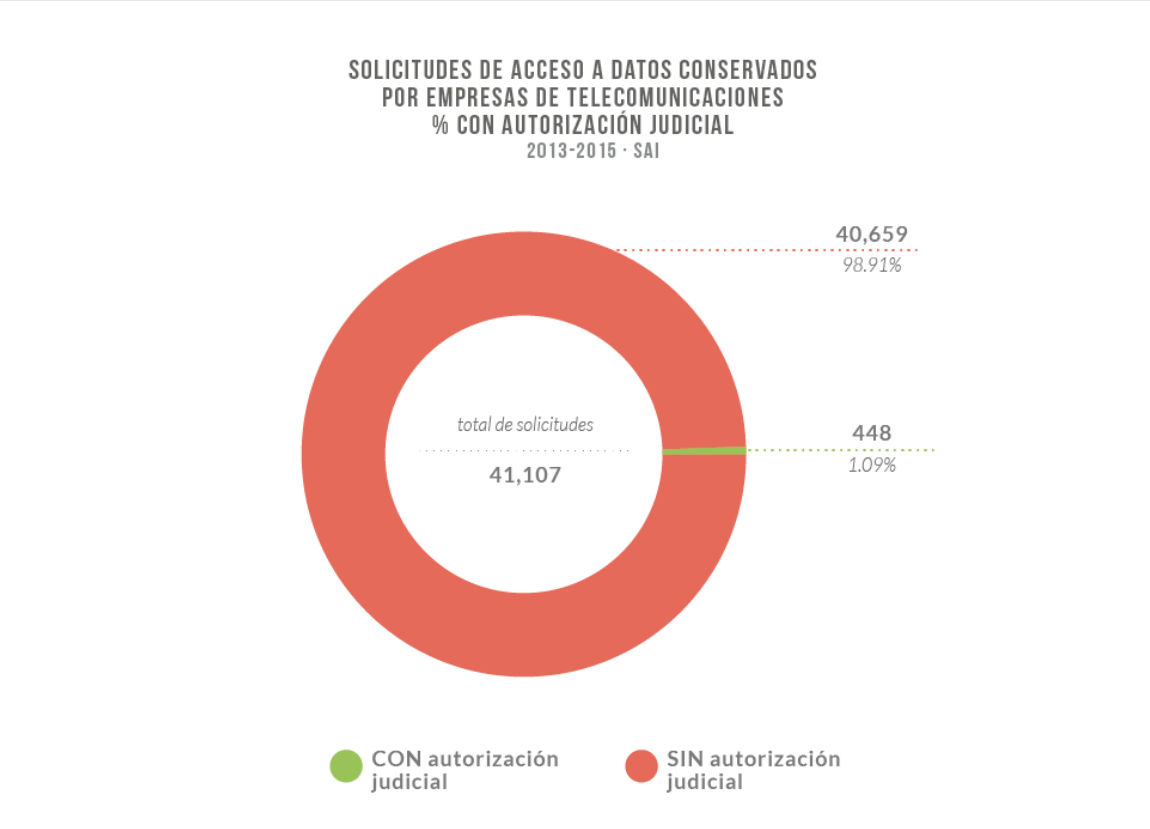
21. En primer lugar, existen graves inconsistencias entre los datos reportados por las autoridades que intervienen comunicaciones privadas y los datos que ofrece el Poder Judicial de la Federación. Por ejemplo, entre 2013 y 2015, las fiscalías y procuradurías de justicia de los Estados de Colima, Zacatecas, Jalisco, Tabasco, Guerrero, Puebla, Querétaro y Quintana Roo reportan haber solicitado la autorización judicial para llevar a cabo intervenciones de comunicaciones privadas. Sin embargo, el Poder Judicial Federal no reporta ninguna solicitud.[12]

22. Igualmente, como muestra la figura a continuación, mientras que el Centro de Investigación y Seguridad Nacional (CISEN) reporta haber realizado 2002 solicitudes de intervención de comunicaciones privadas entre 2013 y 2015, el Poder Judicial únicamente reconoce haber recibido 654. Por el contrario, mientras la Procuraduría General de la República (PGR) reporta haber solicitado la autorización judicial en 866 ocasiones, el Poder Judicial reporta 2392 solicitudes.[13]



[11] Disponible en: https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016.pdf
[12] R3D. Estado de la Vigilancia: Fuera de Control. 2016. Pág. 45.
[13] Ídem.

23. Por otro lado, como aparece en la figura siguiente, se ha documentado que el 98.91% de las veces en las que una autoridad ha accedido a datos de usuarios de telecomunicaciones conservados por las empresas que prestan dichos servicios, lo ha hecho sin una autorización judicial. Lo mismo sucede para el caso de la geolocalización en tiempo real.[14]



24. Inclusive, se han documentado instancias en las que autoridades han accedido a datos de comunicaciones de usuarios sin siquiera poseer facultades legales, como el Tribunal Superior de Justicia de la Ciudad de México, el Gobierno de los Estados de México y de Colima o la Secretaría de Hacienda y Crédito Público.

25. El acceso ilegal a datos de usuarios ha sido facilitado por algunas empresas de telecomunicaciones. Mientras que AT&T rechazó cerca del 46% de las solicitudes que recibió de autoridades por no cumplir con los requisitos legales, el mayor operador, Telcel, no rechazó ninguna de las 87650 solicitudes de acceso a datos de usuarios recibidas en 2016 y el primer semestre de 2017.[15]

26. Además, se ha documentado la ineficiencia de las medidas de vigilancia para la investigación de delitos. Únicamente el 8% de las averiguaciones previas en las que se ha llevado a cabo alguna medida de vigilancia han culminado con

14 Ibidem. Página 56.

15 Dato obtenido de los informes remitidos por Concesionarios y Autorizados en la prestación del servicio de telecomunicaciones al Instituto Federal de Telecomunicaciones correspondientes al año 2016 y el primer semestre de 2017, disponibles en: https://drive.google.com/drive/folders/1DPMpb8LJtF3foQBZaiVd3WwqKOoyfi5R?usp=sharing

el ejercicio de la acción penal.[16] Lo anterior sugiere que más del 90% de las personas vigiladas en el contexto de una investigación criminal no terminan siendo acusadas de ningún delito.

C. Adquisición y operación irregular de *malware* de vigilancia en México

27. 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 programas maliciosos, que permiten a las autoridades extraer información de los dispositivos e incluso tomar su control para convertirlos en un mecanismo de vigilancia permanente.

28. Lo anterior ha sido potenciado por la ausencia de un marco legal que permita supervisar la adquisición y uso de estos programas maliciosos, y la falta de regulaciones en torno a las actividades de 'hacking' por parte del Estado.

29. 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, exponiendo sus clientes y prácticas comerciales.[17]

30. De un total de 35 países, entre los que se encuentran Brasil, Chile, Colombia, Ecuador, Honduras y Panamá, México resultó ser el principal cliente de la firma,[18] con transacciones hechas por parte de diferentes gobiernos locales, dependencias y agencias federales a través de diversas empresas intermediarias.

31. Entre las autoridades mencionadas con relaciones comerciales con Hacking Team se encuentran los Gobiernos de Baja California, Campeche, Chihuahua, Durango, Guerrero, Jalisco, Nayarit, Puebla, Querétaro y Yucatán; la Procuraduría de Justicia del Estado de México; la Secretaría de Seguridad Pública de Tamaulipas; y dependencias federales como la Secretaría de la Defensa Nacional, el Centro de Investigación y Seguridad Nacional, la Policía Federal, la Procuraduría General de la República, e incluso, Petróleos Mexicanos (PEMEX). La gran mayoría de autoridades listadas, ni siquiera posee facultades legales para intervenir comunicaciones privadas, por lo que tanto su adquisición como su uso son claramente ilegales.

32. En agosto de 2016, Citizen Lab,[19] 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*.

16 R3D. Estado de la Vigilancia: Fuera de Control. 2016. Páginas 71-74.

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

18 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/

19 Citizen Lab (2016) About Citizen Lab. Disponible en: https://citizenlab.org/about/

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

34. Existe evidencia de que autoridades mexicanas como la Secretaría de la Defensa Nacional (SEDENA), la Procuraduría General de la República (PGR) y el Centro de Investigación y Seguridad Nacional (CISEN) habrían comprado el software *Pegasus* de NSO. Inclusive, se han revelado graves irregularidades en el proceso de contratación del software *Pegasus* por parte de la PGR.[20] Así como su utilización en contra de defensores de derechos humanos y periodistas como se detalla en el apartado siguiente.

D. Espionaje de periodistas y defensores de derechos humanos en México

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

36. En febrero de 2017, se dio a conocer que el Estado Mexicano utilizó *malware* de vigilancia desarrollado por la empresa israelí NSO Group, con el propósito de espiar a defensores de derechos humanos cuya lucha se enfoca a combatir la obesidad a través del aumento de impuestos a las bebidas azucaradas, incluyendo al director de la organización El Poder del Consumidor. Los ataques perpetrados contra los activistas tuvieron lugar mientras se planeaba una campaña en favor del impuesto a las bebidas azucaradas.[21]

37. En junio de 2017, Citizen Lab, así como ARTICLE 19, la Red en Defensa de los Derechos Digitales (R3D) y SocialTIC publicaron el informe "Gobierno Espía: Vigilancia sistemática a periodistas y defensores de derechos humanos en México",[22] en la cual se da cuenta de múltiples casos de intentos de infección con el malware *Pegasus*.[23]

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

20 MCCI. PGR compró Pegasus a prestanombres. Julio de 2017. https://contralacorrupcion.mx/web/pgrcompropegasus/index.html

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

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

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

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

    - **Centro Miguel Agustín Pro Juárez (Centro Prodh):** Entre los meses de abril y junio del año 2016, tres personas dentro de la organización recibieron mensajes que se ha confirmado constituyen intentos de infección con el malware de espionaje *Pegasus*. Los mensajes fueron recibidos en fechas clave dentro del trabajo de defensa de derechos humanos que el Centro Prodh ha realizado en casos de alto impacto como la desaparición forzada de 43 estudiantes de Ayotzinapa, la masacre de Tlatlaya y los casos de tortura sexual en Atenco.
    - **Aristegui Noticias (Carmen Aristegui, Emilio Aristegui, Rafael Cabrera y Sebastián Barragán):** Se documentaron mensajes recibidos en los años 2015 y 2016 por Carmen Aristegui, por su hijo Emilio y por integrantes de su equipo de investigación como Sebastián Barragán y Rafael Cabrera. En los últimos años, la actividad periodística de Aristegui Noticias ha revelado casos de corrupción como el reportaje de la Casa Blanca[24] o exponer una red de prostitución[25] que operaba desde las oficinas del PRI en la Ciudad de México. Además, ha hecho reportajes sobre casos de violaciones graves a derechos humanos en México como la desaparición forzada de los 43 estudiantes normalistas de Ayotzinapa.[26]

      Es importante enfatizar que, al momento de recibir los mensajes, Emilio era menor de edad. Lo anterior representa el primer ataque documentado con este malware contra un familiar directo de un objetivo y, en total, se fueron contabilizados más de 40 intentos contra el hijo de la periodista.
    - **Carlos Loret de Mola (Periodista):** Periodista de radio, televisión y columnista impreso. Su programa de televisión "Despierta con Loret" (antes "Primero Noticias") es el noticiario con mayor audiencia en el país. Se ha documentado que entre agosto de 2015 a abril de 2016 recibió al menos 8 mensajes que pretendían infectar su dispositivo con el malware *Pegasus*. El primero de los mensajes fue recibido el mismo día que el periodista publicó[27] un reportaje sobre ejecuciones extrajudiciales en Tanhuato, Michoacán.

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

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

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

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

- **Instituto Mexicano por la Competitividad (IMCO):** Se ha documentado que el director de la organización, Juan Pardinas y otra integrante de dicha organización, Alexandra Zapata, recibieron mensajes intentando infectar su dispositivo. IMCO ha sido una de las organizaciones que ha liderado esfuerzos de incidencia para la reforma legal anticorrupción, en particular ha impulsado la ley conocida como "Ley 3 de 3",[28] la cual generó gran resistencia y ataques por parte de fuerzas políticas asociadas al gobierno federal.
- **Mexicanos Contra la Corrupción y la Impunidad (MCCI):** Se ha documentado que los periodistas Salvador Camarena y Daniel Lizárraga, Director General de Investigación Periodística y Jefe de Información de la organización respectivamente, recibió al menos 3 mensajes con malware de NSO en el año 2016. Salvador Camarena y Daniel Lizárraga en el pasado también fueron parte de Aristegui Noticias y participaron en investigaciones como la de revelación de los Panama Papers. Igualmente, el 30 de agosto de 2017 se revelaron ataques con el malware *Pegasus* en contra del director de la organización, Claudio X. González[29] y fueron reveladas otras formas de intimidación por parte del gobierno federal en el periódico *The New York Times*.[30]

40. Aunado a lo anterior, el 10 de julio de 2017 Citizen Lab de la Universidad de Toronto ha confirmado en un nuevo informe, publicado también por el *New York Times*,[32] que un teléfono del Grupo Interdisciplinario de Expertos Internacionales (GIEI) recibió mensajes de texto vinculados a la infraestructura del malware *Pegasus;* el envío de los mensajes de texto con enlaces maliciosos ocurre alrededor de uno de los casos más sensibles para el gobierno federal: la investigación sobre la desaparición forzada de 43 estudiantes (caso Ayotzinapa) lo que confirma la constante obstaculización por parte del gobierno federal en contra del grupo de expertos que puso en tela de juicio la llamada "verdad histórica" de la PGR en el caso Ayotzinapa, además de haber sido objeto de una constante campaña de descalificación para inhibir su labor.

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

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

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

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

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

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

42. El 19 de junio de 2017, 9 de las víctimas de espionaje, acompañadas por organizaciones de la sociedad civil, presentaron una denuncia penal por los hechos revelados en los informes de "Gobierno Espía", exigiendo transparencia en los procesos de contratación de *Pegasus* y una investigación con garantías de independencia.

43. En una de las primeras reacciones oficiales, el Presidente Peña Nieto minimizó la vulneración de la privacidad de todas las personas y amenazó a los denunciantes. Luego de admitir que el gobierno federal ha adquirido el malware Pegasus, el Presidente señaló que "ninguna de las personas que se sienta agraviada puede afirmar o mostrar o evidenciar siquiera que su vida se haya visto afectada por esas supuestas intervenciones y por ese supuesto espionaje".[33]

44. Posteriormente el Presidente Peña Nieto concluyó profiriendo una amenaza en contra de las personas denunciantes al señalar que "espero que la PGR con celeridad pueda deslindar responsabilidades, y espero al amparo de la ley pueda aplicarse contra aquellos que han levantado estos falsos señalamientos".[34]

45. Por otro lado, semanas después de la publicación del informe "Gobierno Espía", en diversos medios de comunicación fueron publicados los contratos, anexos técnicos y otra información relativa a la adquisición de licencias para el uso de *Pegasus* por parte de la Agencia de Investigación Criminal de la PGR.[35] Dentro de la investigación oficial, se ha confirmado que la PGR es usuaria del sistema *Pegasus*, no obstante, el Fiscal encargado del caso se ha negado a requerir los contratos, anexos técnicos o realizar cualquier acto de investigación dirigido a la Agencia de Investigación Criminal.

46. Ante las declaraciones del presidente y ante el hecho de que la PGR, encargada de la investigación oficial, es la principal sospechosa, las y los denunciantes y organizaciones solicitaron que se acepte un mecanismo de supervisión internacional a la investigación, de manera que la sociedad pueda contar con mínimas garantías de que la investigación contará con independencia, exhaustividad y rigor técnico.[36]

47. La gravedad de los hechos denunciados también ha motivado el pronunciamiento de organismos internacionales, por ejemplo, cuatro expertos de la Organización de las Naciones Unidas emitieron un comunicado[37] en el que enfatizaron el deber

[33] Presidente Enrique Peña Nieto. Inauguración de Parque Industrial en Lagos de Moreno, Jalisco. México. 22 de junio de 2017; R3D. Con sus declaraciones, EPN condena al fracaso la investigación por #GobiernoEspía y amenaza a quienes han denunciado. 22 de junio de 2017. Disponible en: https://r3d.mx/2017/06/22/con-sus-declaraciones-epn-condena-al-fracaso-la-investigacion-por-gobiernoespia-y-amenaza-a-quienes-han-denunciado/

[34] Ídem.

[35] Aristegui Noticias. El expediente Pegasus en PGR: radiografía de un sistema de espionaje. Disponible en: http://aristeguinoticias.com/1207/mexico/el-expediente-pegasus-en-pgr-radiografia-de-un-sistema-de-espionaje/

[36] En particular, los autores del presente informe enviaron una carta y un informe al gobierno mexicano, apoyando formalmente la adopción del mecanismo señalado. Disponible en: https://www.privacyinternational.org/advocacy-briefing/994/letter-and-briefing-human-rights-implications-reported-mexican-government

[37] ONU. México: expertos de la ONU piden investigación independiente e imparcial sobre el uso de spyware contra defensores de DD HH y periodistas. Ginebra. 19 de julio de 2017. Disponible en: http://www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?NewsID=21892&LangID=S

de las autoridades mexicanas de garantizar las condiciones necesarias para una investigación transparente, independiente e imparcial sobre las denuncias de la utilización del malware con la intención de espiar a defensores de derechos humanos, activistas y periodistas.

48. Por otra parte, la Iniciativa de las Mujeres Premio Nobel[38] hizo un llamamiento el 17 de julio al gobierno de México para acabar con la vigilancia cibernética y otro tipo de vigilancia sistemática contra los periodistas y activistas, y a poner fin a la criminalización de activistas y periodistas que investigan o enfrentan abusos de los derechos humanos.

49. Al finalizar su visita conjunta a México, los relatores para la libertad de expresión de la ONU y de la CIDH, expresaron su preocupación por el caso y recomendaron asegurar la independencia de la investigación sobre la compra y uso de malware (incluyendo *"Pegasus"*) para vigilar periodistas, activistas y defensores de derechos humanos, así como adoptar medidas legislativas y controles judiciales adecuados para que las medidas de vigilancia se realicen con apego a los derechos humanos, incluso recomendaron que México debería considerar crear un órgano independiente para supervisar de manera efectiva las tareas de vigilancia del Estado.[39]

50. En sentido similar, el relator especial para personas defensoras de derechos humanos Michel Forst emitió su informe tras su visita al país en 2017, en el que señala que la vigilancia secreta a personas defensoras de derechos humanos, es un nuevo y preocupante desafío, especialmente al carecer de medidas adecuadas de control. Respecto a la adquisición de *Pegasus* por parte de las autoridades mexicanas y su aparente uso para vigilar a periodistas y personas defensoras, reiteró su llamamiento y el de otros expertos de las Naciones Unidas para que se lleve a cabo una investigación independiente e imparcial sobre la presunta vigilancia ilegal, al constituir una grave violación de los derechos a la privacidad y las libertades de expresión y asociación.[40]

E. Falta de investigaciòn diligente frente a casos de vigilancia ilegal de periodistas y defensores de derechos humanos

51. A pesar de la gravedad de los hechos, México no ha aceptado el establecimiento de un mecanismo internacional de supervisión y ni siquiera se han hecho públicos los documentos relacionados con la contratación y uso del malware *Pegasus* por parte de agentes del Estado Mexicano.

38 Menchú, Rigoberta. Williams, Betty. Ebadi, Shirin; R3D. Ganadoras del Premio Nobel piden investigación independiente e imparcial sobre el caso #GobiernoEspía. 24 julio de 2017. Disponible en: https://r3d.mx/2017/07/24/ganadoras-del-premio-nobel-piden-investigacion-independiente-e-imparcial-sobre-el-caso-gobiernoespia/

39 Observaciones preliminares del Relator Especial de la ONU sobre la libertad de expresión y el Relator Especial sobre libertad de expresión de la CIDH después de su visita conjunta en México, 27 de noviembre – 4 de diciembre 2017. Disponible en: http://hchr.org.mx/images/doc_pub/ES-final-version-preliminary-observations.pdf

40 Report of the Special Rapporteur on the situation of human rights defenders on his mission to Mexico, 12 de febrero de 2018, A/HRC/37/51/Add.2. Disponible en: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session37/Pages/ListReports.aspx

52. A más de nueve meses del anuncio del inicio de la investigación por parte de la Fiscalía Especial para la Atención de Delitos cometidos contra la Libertad de Expresión (FEADLE) de la PGR, quien está a cargo de la investigación, la investigación no presenta avance alguno. Por el contrario, a pesar de que la representación de las víctimas, bajo la figura de coadyuvante, ha ofrecido o solicitado al menos 70 datos de pruebas, la Fiscalía se ha negado a acordar y llevar a cabo los actos de investigación solicitados por los denunciantes.

53. La Fiscalía ha negado también copia del expediente de investigación a las víctimas y se ha negado a llevar a cabo actos de investigación indispensables, como la identificación de los funcionarios de la PGR capacitados y autorizados para utilizar el sistema *Pegasus*, realizar prácticas forenses en los equipos, servidores y materiales utilizados por los funcionarios de la PGR que operan el sistema *Pegasus* y ni siquiera ha requerido a dicha autoridad los anexos técnicos y otra información sobre el proceso de utilización de *Pegasus* por parte de la PGR.

54. Es importante resaltar que, en el expediente, la Agencia de Investigación Criminal (AIC) de la PGR ha aceptado que adquirió las licencias de uso de *Pegasus* y que el equipo desde el cual se opera dicho software se encuentra ubicado en sus oficinas de la Ciudad de México. Además, el Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia (CENAPI), como la AIC, en su respuesta a la FEADLE, señalan que para la correcta operación del software se tienen contempladas medidas de seguridad internas que contemplan la evaluación periódica y rigurosa del personal por el Centro de Evaluación y Control de Confianza de la PGR, así como medios de encriptación y codificación. Sin embargo, enseguida mencionan que "no se logró identificar una base de datos o expresión documental que contemple el registro de los números que pudieran ser intervenidos".[41]

55. La alegada ausencia de registros sobre el uso de *Pegasus*, pone en evidencia lo señalado inicialmente sobre la ausencia de controles y salvaguardas bajo los que opera la vigilancia en México, sin controles adecuados sobre uso, resulta prácticamente imposible someterlos a una posterior revisión para identificar su correcto uso o en su caso, sancionar arbitrariedades o ilícitos.

56. Por otro lado, la renuencia de parte de la Fiscalía de llevar a cabo actos de investigación respecto de la AIC de la PGR evidencia la falta de autonomía, imparcialidad y profesionalismo en la investigación, especialmente dado que tanto la autoridad que lleva a cabo la investigación, la FEADLE, como la única autoridad que ha aceptado el uso del malware *Pegasus*, la AIC, forman parte de la misma PGR.

[41] CARPETA DE INVESTIGACIÓN FED/SDHPDSC/UNAI-CDMX/0000430/2017, Oficio de respuesta de la AIC de fecha 14 de agosto de 2017 - PGR/AIC/0430/2017, Oficio de respuesta de la CENAPI de fecha 14 de agosto de 2017, PGR/AIC/CENAPI/OT/DGAAJ/10077/2017

57. Como han señalado a *The New York Times*[42] expertos forenses y la propia empresa fabricante del malware, NSO Group, un análisis forense de los servidores y equipos desde los que se opera el sistema *Pegasus* debería poder encontrar un registro de las infecciones realizadas con ese sistema. La Fiscalía se ha negado a hacer cualquier acto de investigación al respecto.

58. En un sentido similar, las investigaciones anunciadas por parte del Instituto Nacional de Acceso a la Información y Protección de Datos Personales (INAI) y por la Comisión Nacional de Derechos Humanos (CNDH) no han representado avances significativos, en parte, según ha sido revelado por dichas instituciones, debido a la obstaculización de sus diligencias por parte de la PGR.

RECOMENDACIONES

59. Recomendamos que el Estado Mexicano:

1. Establezca un grupo internacional de expertos que investigue de manera autónoma e independiente los casos de vigilancia ilegal de periodistas y defensores de derechos humanos.

2. Investigue diligentemente y sancione a los responsables intelectuales y materiales del espionaje ilegal a periodistas y defensores de derechos humanos con el malware *Pegasus*.

a. La Fiscalía a cargo de la investigación oficial debe llevar a cabo todos los actos de investigación que resulten necesarios, como la identificación e investigación de todos los funcionarios de la Agencia de Investigación Criminal de la PGR que fueron capacitados para operar el sistema *Pegasus* o que participaron de cualquier manera en el proceso de selección de objetivos, en la operación y en el procesamiento de la inteligencia obtenida mediante ese sistema. Igualmente es indispensable que se realicen prácticas forenses en los equipos e instalaciones de la Agencia de Investigación Criminal destinados a la operación del sistema *Pegasus*.

b. Disponer una política de cooperación irrestricta de todos los órganos estatales con las investigaciones llevadas a cabo por órganos autónomos como el INAI y la CNDH, así como con el grupo internacional de expertos que sea establecido.

c. Transparentar proactivamente toda la información relativa a los procesos de contratación, incluyendo información técnica sobre las capacidades de vigilancia adquirida, celebrados entre las dependencias federales

[42] Ahmed, Azam, EE. UU. y las víctimas de Pegasus desestiman la investigación de espionaje, New York Times, 20 de febrero de 2018. Disponible en: https://www.nytimes.com/es/2018/02/20/mexico-fbi-investigacion-pegasus-espionaje/?action=click&clickSource=inicio&contentPlacement=1&module=toppers&region=rank&pgtype=Homepage

y estatales y cualquier empresa, con el objeto de adquirir equipos o licencias de uso de herramientas de vigilancia e intervención de comunicaciones privadas, reservando sólo informaciones específicas que de manera demostrable pongan en serio riesgo una investigación, amenace la vida o integridad de una persona.

d. Notificar a todos las personas que han sido objeto de ataques intrusivos hasta la fecha, incluyendo la base legal y normas pertinentes, si los hubiere, que rigen dichas actividades, o destruir todo el material obtenido a través de sus ataques intrusivos, ofreciendo a todos los personas que han sido objeto de sus ataques de intrusivos una vía de reparación efectiva.

3. Legisle e implemente las reformas necesarias para garantizar que la adquisición y operación de herramientas de vigilancia se lleve a cabo de manera legal, necesaria, proporcional y respetuosa de los derechos humanos.

a. El Código Nacional de Procedimientos Penales, la Ley Federal de Telecomunicaciones, la Ley de la Policía Federal, la Ley de Seguridad Nacional, la Ley Federal para Prevenir y Sancionar los Delitos en Materia de Secuestro, la Ley contra la Delincuencia Organizada y el Código Militar de Procedimientos Penales deben ser reformadas con el objeto de:

- Establecer con claridad y precisión las autoridades facultadas, las circunstancias y los procedimientos para intervenir comunicaciones privadas y acceder a los datos de comunicaciones (metadatos), así como para llevar a cabo la localización geográfica en tiempo real de equipos de comunicación.
- Establecer explícitamente la necesidad de contar con una autorización judicial previa y debidamente fundada para llevar a cabo medidas de vigilancia, salvo casos de emergencia en los que el control judicial deberá ser inmediato.
- Otorgar facultades efectivas de fiscalización y supervisión de los sistemas de vigilancia a una autoridad independiente, como pueden ser el Instituto Nacional de Acceso a la Información y Protección de Datos Personales o la Comisión Nacional de Derechos Humanos
- Reconocer el derecho de toda persona a ser notificado de injerencias estatales en su vida privada. Dicha notificación solamente podrá ser diferida cuando de manera demostrable dicha notificación obstaculice seriamente una investigación o ponga en riesgo la vida o integridad física de una persona.

b. Regular la adquisición y operación de herramientas de vigilancia intrusiva, implementando las siguientes salvaguardas para garantizar que estas actividades sean practicadas acorde a un enfoque de derechos humanos:

- **Legalidad:** las facultades de vigilancia deben estar autorizadas por una ley cpm límites claros y precisos.

- **Seguridad e integridad de los sistemas:** debe realizarse una evaluación sobre los riesgos y daños a la seguridad e integridad de las comunicaciones antes de llevar a cabo estas medidas.
- **Necesidad y proporcionalidad:** deben establecerse factores que permitan medir la probabilidad de ocurrencia de una amenaza contra un bien público protegido, información sobre el método, alcance y duración de la medida propuesta, y una evaluación de la seguridad.
- **Autorización judicial:** una autoridad imparcial e independiente debe decidir si aprueba o no la medida y supervisar su aplicación, incluyendo la posibilidad de consultar a expertos técnicos y de otras áreas.
- **Integridad de la información:** las autoridades gubernamentales no pueden añadir, alterar o borrar datos recolectados a través de la medida de intervención.
- **Notificación:** las autoridades gubernamentales deben notificar a las personas sujetas de vigilancia las circunstancias relativas a la medida.
- **Destrucción y devolución de datos:** las autoridades gubernamentales deben establecer un procedimiento de destrucción de datos irrelevantes a la investigación, además de establecer un registro de este procedimiento.
- **Supervisión y transparencia:** las autoridades deben someter sus facultades y actividades a un organismo de supervisión que sea independiente de los servicios de inteligencia y del gobierno, debiendo publicar información relacionada con las solicitudes.
- **Extraterritorialidad:** las autoridades deben cumplir sus obligaciones legales y abstenerse de utilizar medidas de cooperación internacional para eludir mecanismos legales.
- **Remedios:** las personas sujetas a las medidas de intervención estatal ilegal deben tener acceso a un recurso efectivo.

4. **Derogue o se abstenga de aprobar legislación que contenga disposiciones en materia de vigilancia e intervención de comunicaciones privadas que:**

   a. Omitan señalar con precisión las autoridades facultadas para llevar a cabo medidas de vigilancia, faculte a autoridades no autorizadas por la Constitución o faculte a autoridades distintas de las civiles.

   b. Establezcan medidas de vigilancia masiva.

   c. Omitan establecer con precisión y claridad las circunstancias y procedimientos que deben seguirse para llevar a cabo medidas de vigilancia.

d. No contengan controles democráticos y medidas de rendición de cuentas como el control judicial previo o inmediato, la supervisión independiente, la transparencia y el derecho de notificación.

5. **Elimine las obligaciones de conservación masiva e indiscriminada de metadatos de comunicaciones contempladas en el artículo 190, fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión.**