EJÉRCITO ESPÍA

CENTRO PRODH NUEVAMENTE ATACADO CON PEGASUS:

CÓMO LA IMPUNIDAD Y LA MILITARIZACIÓN PROPICIARON LA REPETICIÓN DEL ESPIONAJE

Centro Prodh
CENTRO DE DERECHOS HUMANOS MIGUEL AGUSTÍN PRO JUÁREZ A.C.

R3D
Red en Defensa de los Derechos Digitales

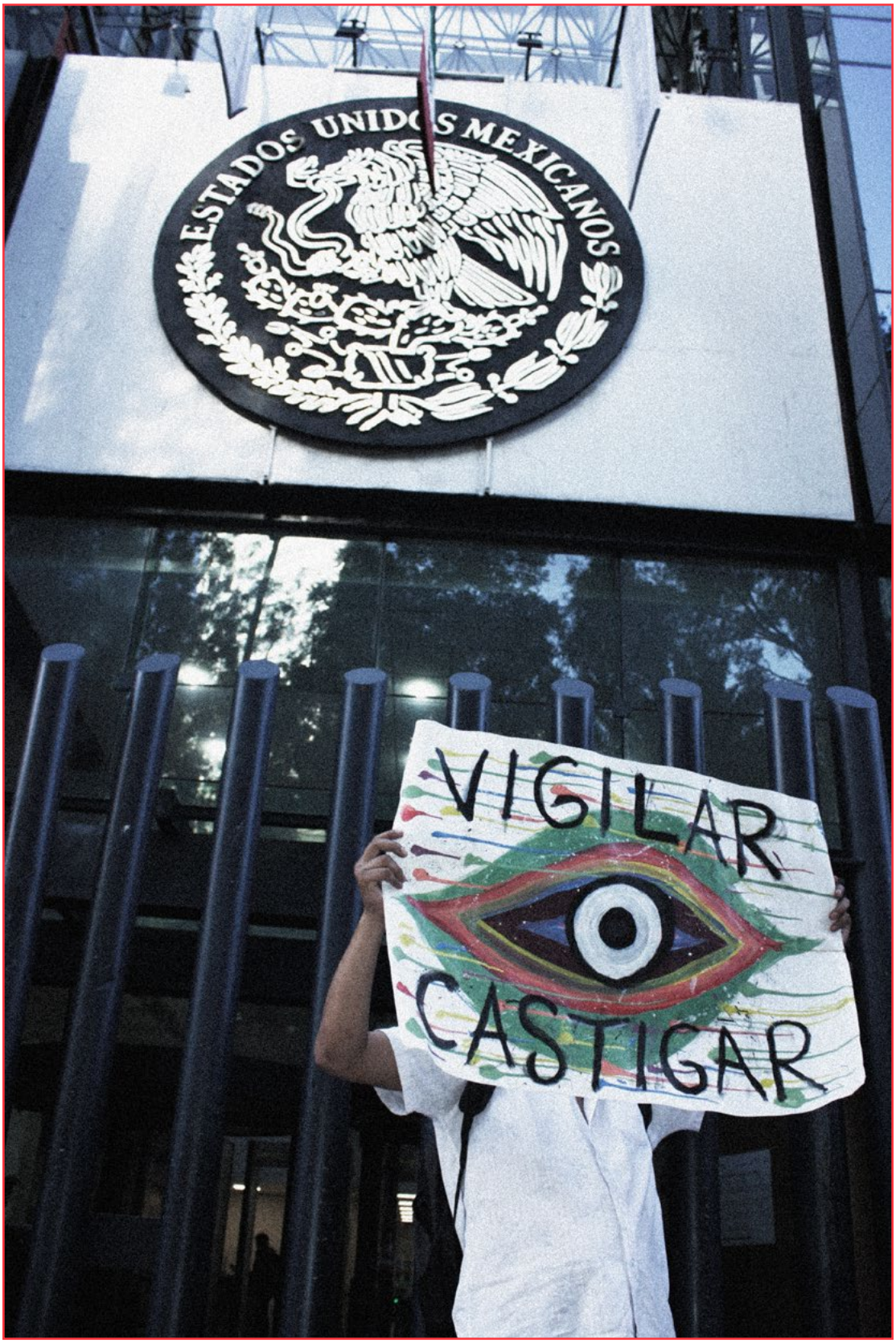
SOCIAL TIC

ARTICLE 19

EJÉRCITO ESPÍA. CENTRO PRODH NUEVAMENTE ATACADO CON PEGASUS: CÓMO LA IMPUNIDAD Y LA MILITARIZACIÓN PROPICIARON LA REPETICIÓN DEL ESPIONAJE

Ciudad de México. México, Abril 2023.

ÍNDICE


ESTADOS UNIDOS MEXICANOS
VIGILAR
CASTIGAR

INTRODUCCIÓN

Desde el año 2017, la Red en Defensa de los Derechos Digitales (R3D), ARTICLE 19 y SocialTIC, organizaciones dedicadas a la defensa de los derechos humanos en el entorno digital, la libertad de expresión y la promoción de la tecnología digital respectivamente, en colaboración con Citizen Lab, de la Universidad de Toronto, hemos documentado múltiples casos de intervención ilegal de comunicaciones privadas a través del *malware Pegasus*, desarrollado por la empresa israelí NSO Group a través de investigaciones como "Gobierno Espía" y "Ejército Espía".

En este informe, publicamos nueva información que demuestra la existencia de ataques con *Pegasus* durante el año 2022 en contra del Centro de Derechos Humanos Miguel Agustín Pro Juárez (Centro Prodh), organización fundada por la Compañía de Jesús hace 35 años y desde entonces dedicada al acompañamiento y defensa integral de graves violaciones a derechos humanos. El Centro Prodh ha sido objeto de espionaje con *Pegasus* en dos ocasiones y administraciones distintas, ambas en contextos vinculados con el trabajo de exigencia de verdad y justicia para las víctimas que acompaña.

El espionaje más reciente se da después de que la Fiscalía General de la República (FGR) no fue capaz de investigar y esclarecer la denuncia de espionaje ocurrida en el gobierno pasado (2017), y ante un contexto de empoderamiento de las Fuerzas Armadas.

EL *MALWARE* PEGASUS

En agosto de 2016, Citizen Lab, el laboratorio interdisciplinario de la escuela Munk de Asuntos Globales de la Universidad de Toronto, en Canadá, publicó información inédita sobre un poderoso software de vigilancia llamado *Pegasus*, comercializado por la empresa NSO Group Technologies fundada en 2010 y dedicada a la comercialización de tecnologías de vigilancia, que según afirma son utilizadas exclusivamente para clientes gubernamentales aprobados por el Ministerio de Defensa de Israel.

Cuando un dispositivo móvil es infectado con *Pegasus*, el atacante adquiere la posibilidad de acceder a toda la información almacenada, como mensajes, correos y contactos; obtener el registro de cada tecla oprimida; acceder a llamadas, monitorear datos de localización; la posibilidad de recolectar información mediante la activación secreta del micrófono o la cámara así como obtener contraseñas; además, *Pegasus* permite al operador acceder a conversaciones y llamadas incluso mediante plataformas encriptadas. Es decir, el atacante

obtiene prácticamente un control absoluto sobre el dispositivo y su contenido. Pese a que NSO Group afirma respetar una política de derechos humanos, de acuerdo con Citizen Lab, el número de casos documentados en los que su tecnología se utiliza de forma abusiva contra la sociedad civil sigue creciendo.

En las primeras investigaciones sobre el uso de *Pegasus* en México, el principal método de infección consistía en el envío de mensajes de texto (SMS) con información de interés para las personas-objetivo acompañados con enlaces (URL). El objetivo del atacante era el de provocar el clic en el enlace, pues, de esta manera es que el programa *Pegasus* era instalado. Citizen Lab también estableció la dificultad de encontrar rastro del espionaje en el dispositivo en ese entonces, debido a las medidas anti forenses que posee.

Ejemplos de mensajes de texto recibidos por el Centro Prodh en 2016, con enlaces maliciosos hacia la infraestructura de NSO Group.

Actualmente, la infección con *Pegasus* no requiere dar clic en ningún enlace, sino que se introduce directamente al celular aprovechándose de alguna vulnerabilidad del sistema operativo o alguna aplicación del dispositivo (*zero click exploit*). Ello facilita que el malware acceda al dispositivo que busca infectar, y para la persona objeto del espionaje, es más difícil saber que su información y comunicaciones han quedado vulneradas.

El uso de *Pegasus* en contra de periodistas, personas defensoras de derechos humanos, activistas y opositores ha sido ampliamente documentada alrededor del mundo. Por ejemplo, se documentó el espionaje a un periodista estadounidense del *New York Times* ubicado en Líbano. En Panamá fue ampliamente conocido el espionaje a opositores, empresarios y activistas del que se acusó al entonces presidente Martinelli; también se han documentado casos de espionaje a opositores políticos en Togo, a periodistas y activistas en India, defensores de derechos humanos en Marruecos, disidentes políticos y a periodistas de Arabia Saudita, uno de ellos, Jamal Khashoggi, fue espiado antes de ser brutalmente asesinado. Igualmente, han sido documentados casos de abuso en Hungría, India, Polonia, España, entre otros casos alrededor del mundo, como aquellos publicados como parte de la investigación "Pegasus Project".

La documentación de abusos derivó en múltiples investigaciones y procesos judiciales. Por ejemplo, existen diversas demandas en contra de la empresa NSO Group en Chipre e Israel, por su negligencia frente a los abusos cometidos en el uso de *Pegasus*, incluyendo México. Además, en Estados Unidos se siguen procesos en contra de la empresa NSO Group por el ataque a plataformas como WhatsApp y Apple para cometer espionaje en contra de defensores y periodistas. A raíz de los abusos con el malware *Pegasus*, el Departamento de Comercio de Estados Unidos incluyó a NSO Group en una lista de sanciones, con lo cual la empresa se encuentra impedida de acceder a tecnologías estadounidenses. Además, recientemente el Presidente de dicho país emitió una orden ejecutiva que prohíbe a todas las agencias del gobierno el uso de programas de espionaje comerciales que impliquen riesgos a la Seguridad Nacional o que se encuentren vinculadas a violaciones a derechos humanos.

ANTECEDENTES DE PEGASUS EN MÉXICO: PRIMEROS CASOS DOCUMENTADOS Y DENUNCIADOS

El primer antecedente de *Pegasus* en México se registró en el año 2011, cuando investigaciones periodísticas publicaron que la Secretaría de la Defensa Nacional (Sedena), se convirtió en el primer cliente internacional de NSO Group al adquirir el sistema *Pegasus* como parte de una serie de contratos celebrados con la empresa Security Tracking Devices S.A. de C.V., los cuáles ascendieron a 5.6 mil millones de pesos. Dichas

contrataciones sucedieron luego de una demostración de cómo funciona el sistema *Pegasus*, al entonces presidente, Felipe Calderón, y al Secretario de Defensa Nacional, Guillermo Galván Galván, en mayo de 2011.

Posteriormente, tras una investigación publicada por Citizen Lab en 2016 se encontró que la mayoría de los nombres de dominio que la infraestructura de NSO Group, que utilizaba para infectar dispositivos con *Pegasus*, se encontraban vinculados a México, lo que llevó a investigadores y organizaciones a presumir que autoridades mexicanas eran clientes de NSO y que personas en México podrían haber sido objetivos de vigilancia.

A raíz de las investigaciones emprendidas por organizaciones de la sociedad civil en México –en colaboración con Citizen Lab– se documentaron múltiples casos de ataques con *Pegasus* en contra de periodistas y personas defensoras de derechos humanos en México. Reportajes publicados por el New York Times el 11 de febrero de 2017 y 19 de junio de 2017, retomaron y acompañaron la publicación del informe #GobiernoEspía: vigilancia sistemática a periodistas y defensores de derechos humanos.

Presentación del informe *Gobierno Espía: Vigilancia sistemática a periodistas y defensores de derechos humanos en México*. 19 de junio de 2017.

Éste fue dado a conocer el 19 de junio de 2017 por las organizaciones ARTICLE 19 Oficina para México y Centroamérica, R3D: Red en Defensa de los Derechos Digitales, y SocialTIC, junto con los reportes del laboratorio Citizen Lab, en el que se documentó que, entre enero de 2015 y julio de 2016, se habían enviado más de 70 mensajes de texto con vínculos hacia la infraestructura de *Pegasus*, dirigidos a 12 periodistas y defensores de derechos humanos en México, entre ellos, el equipo de *Aristegui Noticias*, integrantes del Poder del Consumidor, de Mexicanos contra la Corrupción y la Impunidad (MCCI), del Instituto Mexicano para la Competitividad, A.C. (IMCO), así como tres integrantes del Centro de Derechos Humanos Miguel Agustín Pro Juárez (Centro Prodh). Posteriormente, se sumaría el espionaje realizado a integrantes del Grupo Interdisciplinario de Expertos Independientes (GIEI) del caso Ayotzinapa. Para marzo de 2019 se sumaban 25 casos de espionaje en México documentados por Citizen Lab.

Investigaciones periodísticas y de las organizaciones de la sociedad civil, verificaron que autoridades mexicanas como SEDENA, el entonces Centro de Investigación y Seguridad Nacional (CISEN) y la entonces Procuraduría General de la República (PGR), mediante la Agencia de Investigación Criminal (AIC), habían comprado este software. La última fue acreditada, tras una investigación ministerial.

La corrupción asociada con la compra de *Pegasus* ha sido otra vertiente relevante. Investigaciones periodísticas han permitido establecer que la tecnología desarrollada por NSO Group fue adquirida por autoridades mexicanas a través de empresas nacionales de reciente creación, las cuales fungieron como intermediarias y que se beneficiaron de millonarias asignaciones directas, aun cuando carecían de experiencia acreditable en el campo de la seguridad nacional, lo cual fue difundido en investigaciones periodísticas en la revista *Proceso* y Mexicanos contra la Corrupción y la Impunidad. Esto incluso generó un exhorto del Comité de Participación Ciudadana del Sistema Nacional Anticorrupción (SNA), que posteriormente rechazada por el Comité Coordinador del SNA.

Desde que se hicieron públicos los casos de espionaje en México, se exigió la transparencia, en versión pública, de todos los contratos que se hubieran celebrado para la adquisición de *Pegasus* por autoridades mexicanas, lo que después se formalizó en la carpeta ante FGR. Incluso fue necesario llevar a cabo diversos litigios para obligar al Instituto Nacional de Acceso a la Información Pública (INAI) a ordenar la publicación de los contratos celebrados por la PGR en 2014, 2016 y 2017.

En el caso del Centro Prodh, meses antes de que se descubriera el espionaje, se filtró en medios de comunicación una llamada sostenida entre uno de los integrantes de este centro de derechos humanos y un familiar de Ayotzinapa, la cual fue utilizada de forma manipulada y tendenciosa.

LA IMPUNIDAD FRENTE A LAS DENUNCIAS DE ESPIONAJE

El 19 de junio de 2017, luego de que se hicieran públicos los casos de espionaje en contra de personas defensoras y periodistas, algunas de las víctimas, incluyendo los integrantes del Centro Prodh, presentaron una denuncia penal ante la Fiscalía Especial para la Atención de Delitos cometidos contra la Libertad de Expresión (FEADLE) de la Subprocuraduría de Derechos Humanos, Prevención del Delito y Servicios a la Comunidad (SDHPDSC) de la entonces Procuraduría General de la República (PGR), por los delitos de intervención de comunicaciones privadas, acceso ilícito a sistemas y equipos de informática y los que resulten, y se inició la carpeta de investigación FED/SDHPDSC/UNAI-CDMX/0000430/2017.

Pese al llamado de múltiples instancias, nacionales e internacionales (como la Oficina del Alto Comisionado de la ONU para los Derechos Humanos (ONU-DH) y Procedimientos Especiales de la ONU, la Comisión Interamericana de Derechos Humanos (CIDH), entre otros[1]) respecto a la necesidad de llevar a cabo una investigación diligente y con garantías reforzadas de autonomía, ya que la investigación, hasta la fecha, no ha permitido el esclarecimiento de los hechos.

Por el contrario, la FGR ha requerido que las propias víctimas sean quienes aporten pruebas (como contratos, informes técnicos de Citizen Lab, notas periodísticas sobre la adquisición del *malware* y los intermediarios, entre otras), y que sean ellas quienes tengan que acudir ante autoridad judicial para solicitar, mediante audiencia de tutela de derechos[2], que las pruebas y diligencias sean admitidas (por ejemplo, los contratos y facturas solicitadas a distintas dependencias, información sobre las dependencias y empresas intermediarias, la revisión de los servidores de *Pegasus* y la realización de entrevistas a operadores, entre otras). También se ha exigido que se atienda la totalidad de las líneas de investigación, incluyendo la posible corrupción en la compra de *Pegasus*, y la posible obstrucción de la investigación señalada por el INAI.

Pese a la desconfianza y con la finalidad de impulsar la investigación, algunas de las personas denunciantes acudieron a la FGR a aportar información sensible: como los registros de comunicaciones que

[1] 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/; Posicionamiento del Comité de Participación Ciudadana sobre acusaciones de espionaje a periodistas, activistas sociales y defensores de derechos humanos, http://cpc.org.mx/2017/06/22/posicionamiento-del-comite-de-participacion-ciudadana-sobre-acusaciones-de-espionaje-a-periodistas-activistas-sociales-y-defensores-de-derechos-humanos/

[2] Primera audiencia ante Juez de Control celebrada el 21 de mayo de 2018. Segunda audiencia ante Juez de Control, de 17 de mayo de 2019.

corroboraban la recepción de mensajes SMS con enlaces, con el objetivo de infectar los dispositivos con el *malware Pegasus*.

En la carpeta se presentó la evidencia técnica aportada por Citizen Lab, así como la ruta que los expertos internacionales sugerían para desarrollar la investigación[3], la cual estaba dirigida prioritariamente a la revisión de equipos, infraestructura, servidores y documentación de las entidades gubernamentales que utilizan *Pegasus*. Lamentablemente, lejos de atender esta ruta, la FGR se centró por muchos años en requerir a las víctimas sus dispositivos para analizar si estos se encontraban o no infectados.

Pese a las expectativas generadas por el cambio de administración y por la transición de la PGR a la FGR, la deficiente aproximación al caso por parte de la dependencia continuó y repercutió en un limitado entendimiento de las nuevas autoridades sobre el caso, sus dimensiones técnicas y sus alcances. Las principales falencias registradas en la investigación han sido: i) la ausencia de un plan de investigación completo, integral y abarcativo; ii) la falta de seguimiento respecto de actos de investigación propuestos por la coadyuvancia; iii) el no agotamiento de nuevas líneas de investigación aportadas por el equipo de periodistas víctimas; iv) la aproximación técnica deficiente por la ausencia de capacidades periciales; v) la obstrucción a la investigación; y vi) la fragmentación de la indagatoria.

La única expresión de proactividad registrada en la carpeta de investigación, se dio como respuesta de las autoridades a la investigación realizada a nivel internacional denominada "*Pegasus Project*", que motivó la judicialización de la investigación a partir de información que fue aportada por el equipo de *Aristegui Noticias*. Ésta hacía referencia a la red de intermediarias que, durante el anterior sexenio, crearon una estructura paralela: por medio de actores privados comercializaban y participaban en la operación de *Pegasus* por instrucciones de autoridades del más alto nivel de la anterior administración para favorecer sus intereses.

[3] Entre ellas: a) la auditoría de los dispositivos o equipos de Pegasus del gobierno, para obtener: materiales de auditoría y los registros de cada implementación del *malware*, imagen forense de cada disco duro del servidor *Pegasus*, registros del servidor, *firewall* y conexión, así como los registros de actualización para todas las implementaciones de *Pegasus*; b) El análisis de infraestructura de las entidades en el gobierno que operan Pegasus, para obtener: una lista de todos los servidores utilizados por sus clientes, los recibos de facturación y otras informaciones sobre los dominios y el alojamiento que se compraron para las implementaciones de *Pegasus* en México; c) El análisis de la documentación de la relación contractual entre el gobierno mexicano con NSO Group, para obtener: lista de todas las personas que han recibido capacitación sobre cómo operar *Pegasus*, y la lista de a quién reportan (línea jerárquica de toma de decisiones) y los materiales de capacitación escritos y grabados provistos por NSO Group con respecto a la operación de Pegasus.

La información mencionada derivó en la detención de una persona, a quien se le vinculó a proceso por el delito de intervención de comunicaciones, por su probable participación en el espionaje como operador del *software* dentro de una de las empresas intermediarias entre NSO y PGR. A la fecha, no se ha llevado a cabo la audiencia del juicio respecto a la única persona detenida. Peor aún, no se ha avanzado en otras responsabilidades de las autoridades e instituciones: tanto por el uso de *Pegasus* por sí mismas (a través por ejemplo de la AIC de PGR), así como por las posibles instrucciones realizadas a empresas privadas intermediarias (línea de investigación que se seguiría tras la detención). Tampoco se ha avanzado en la investigación asociada a la compra del software mediante esquemas de corrupción, y a las múltiples contradicciones y obstrucciones registradas. En estas circunstancias, la relevancia que habría podido tener la detención y vinculación a proceso referida, se diluye ante la falta de esclarecimiento de los hechos y de sanción a todas las responsabilidades asociadas con el espionaje.

Dada la gravedad de los hechos, la FGR estaba obligada a realizar una investigación pronta, exhaustiva, independiente e imparcial para que los responsables materiales e intelectuales fueran identificados y llevados ante la justicia, al tiempo de conocer cómo operó el espionaje, y, con ello, contribuir a que los abusos cometidos con relación a la adquisición y uso ilegal del *software Pegasus* no se repitieran. Sin embargo, ello no ocurrió, y, no solo ha faltado a su obligación de acercar verdad y justicia a las víctimas, sino que ha perpetuado la impunidad y generado las condiciones para la repetición de los hechos.

ESPIONAJE CON *PEGASUS* EN EL ACTUAL GOBIERNO

Pese al cambio de gobierno y las reiteradas declaraciones por parte del titular del Ejecutivo sobre que el espionaje a periodistas y personas defensoras de derechos humanos ya no ocurriría y que ya no se operaría *Pegasus* ni ningún otro sistema de intervención de comunicaciones privadas similar, esto no ocurrió. En fechas recientes se ha revelado evidencia sobre nuevos casos de espionaje a través de *Pegasus* atribuibles con un alto grado de certeza al Ejército mexicano. La información documentada por las organizaciones se puede consultar en https://ejercitoespia.mx/

El 2 de octubre de 2022, en una primera publicación de evidencia validada por Citizen Lab, se dio cuenta del espionaje con *Pegasus* en contra del periodista Ricardo Raphael, un periodista del medio *Animal Político*, y del defensor de Derechos Humanos Raymundo Ramos.

Las infecciones con *Pegasus* detectadas ocurrieron durante los años 2019, 2020 y 2021 en momentos en donde los periodistas y la persona defensora de derechos humanos llevaban a cabo labores relacionadas con

violaciones a derechos humanos cometidas por las Fuerzas Armadas. Además, el análisis forense realizado por Citizen Lab detectó que, a diferencia de los casos detectados en el gobierno anterior, las infecciones ocurrieron mediante el aprovechamiento de vulnerabilidades en dispositivos Apple que no requirieron que el blanco del ataque tuviera que dar clic a algún enlace o realizar ninguna acción para provocar la infección (*zero click exploit*).

El defensor de derechos humanos Raymundo Ramos (centro), junto con el analista político Ricardo Raphael (izq.) y el periodista Daniel Moreno, durante la presentación de la investigación *Ejército Espía*. 3 de octubre de 2022.

La investigación, además, reveló información que señalaba al Ejército como el probable responsable de realizar el espionaje. Destaca un documento interno de la SEDENA con número de oficio SGE-3335 dirigido al Secretario de la Defensa Nacional, obtenido por el Colectivo Guacamaya, que demuestra la celebración de un contrato entre la SEDENA y la empresa Comercializadora Antsua S.A. de C.V. identificado como DN-10 SAIT 1075/P/2019, celebrado en abril de 2019, cuyo objeto fue la adquisición de un "Servicio de Monitoreo Remoto de Información".

La empresa Comercializadora Antsua S.A. de C.V. había sido identificada previamente como parte del entramado comercial que fue utilizado para realizar la adquisición de licencias de *Pegasus* por parte de la PGR, el CISEN y la propia SEDENA durante el gobierno de Enrique Peña Nieto. Por ejemplo, ha sido publicada eviden-

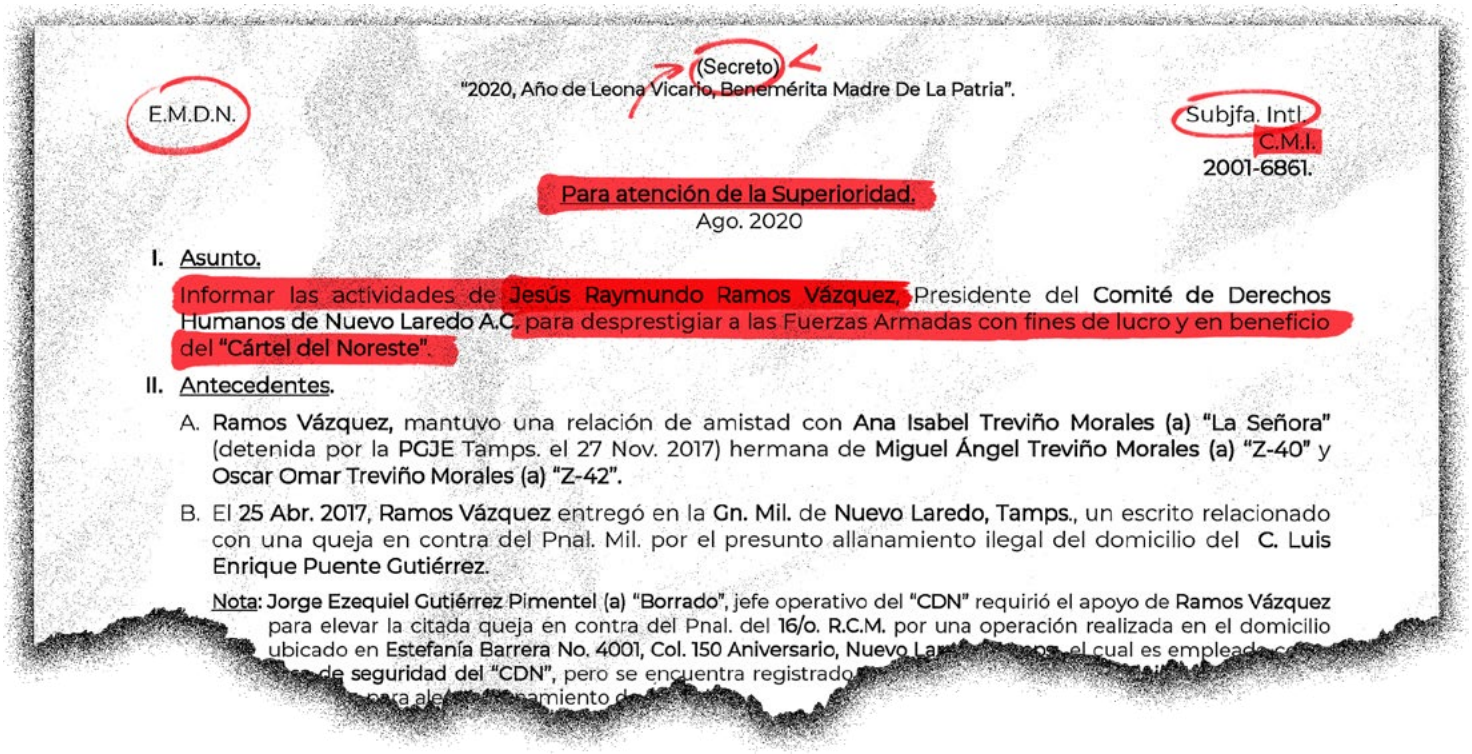
cia de que una persona que funge como apoderada legal de Comercializadora Antsua, fungió como comisario e integrante del órgano de vigilancia de Proyectos y Diseños VME S.A. de C.V. empresa utilizada durante el gobierno de Peña Nieto para comercializar licencias de *Pegasus*.

Según ha sido reportado, documentos obtenidos a partir de un cateo a las oficinas de Proyectos y Diseños VME indican que Comercializadora Antsua fue autorizada por NSO Group para representarla exclusivamente ante la SEDENA, al menos hasta diciembre de 2019. Además, previamente había sido publicada una factura pagada en 2016 por la SEDENA a Proyectos y Diseños VME por un contrato cuyo objeto era un "Servicio de Monitoreo Remoto de Información", mismo objeto que el contrato de 2019 entre la SEDENA y Comercializadora Antsua. También fue publicada una transferencia de Proyectos y Diseños VME a NSO Group, presumiblemente producto de las contrataciones durante el gobierno de Peña Nieto.

La investigación también demostró cómo la SEDENA ocultó las contrataciones y realizó declaraciones falsas ante la carpeta de investigación abierta por la FGR, ante requerimientos de la Auditoría Superior de la Federación y ante solicitudes de acceso a la información. No obstante, documentos internos de la SEDENA obtenidos por R3D mediante solicitudes de acceso a la información realizadas a la Auditoría Superior de la Federación corroboraron que la SEDENA admitió, a través de una tarjeta informativa, la celebración del contrato con Comercializadora Antsua S.A. de C.V. y la realización de pagos que ascendieron a cerca de 140 millones de pesos de abril a diciembre de 2019.

Luis Fernando García, director de R3D: Red en Defensa de los Derechos Digitales, presenta las evidencias de la investigación *Ejército Espía*. 3 de octubre de 2022.

Una segunda entrega de la investigación "Ejército Espía", publicada el 7 de marzo de 2023, añadió información que demuestra de manera contundente que la SEDENA fue la Institución que realizó la infección con *Pegasus* en contra del defensor de derechos humanos Raymundo Ramos.



(Secreto)

"2020, Año de Leona Vicario, Benemérita Madre De La Patria".

E.M.D.N.

Subjfa. Intl.
C.M.I.
2001-6861.

Para atención de la Superioridad.
Ago. 2020

I. Asunto.

Informar las actividades de **Jesús Raymundo Ramos Vázquez**, Presidente del **Comité de Derechos Humanos de Nuevo Laredo A.C.** para desprestigiar a las Fuerzas Armadas con fines de lucro y en beneficio del **"Cártel del Noreste"**.

II. Antecedentes.

A. **Ramos Vázquez,** mantuvo una relación de amistad con **Ana Isabel Treviño Morales (a) "La Señora"** (detenida por la PGJE Tamps. el 27 Nov. 2017) hermana de **Miguel Ángel Treviño Morales (a) "Z-40"** y **Oscar Omar Treviño Morales (a) "Z-42".**

B. El **25 Abr. 2017, Ramos Vázquez** entregó en la **Gn. Mil.** de **Nuevo Laredo, Tamps.**, un escrito relacionado con una queja en contra del Pnal. Mil. por el presunto allanamiento ilegal del domicilio del **C. Luis Enrique Puente Gutiérrez.**

Nota: **Jorge Ezequiel Gutiérrez Pimentel (a) "Borrado"**, jefe operativo del **"CDN"** requirió el apoyo de **Ramos Vázquez** para elevar la citada queja en contra del Pnal. del **16/o. R.C.M.** por una operación realizada en el domicilio ubicado en **Estefanía Barrera No. 4001, Col. 150 Aniversario, Nuevo La** el cual es empleado **de seguridad del "CDN"**, pero se encuentra registrado

Extracto de la nota informativa del Centro Militar de Inteligencia donde se consigna el espionaje al defensor Raymundo Ramos en agosto-septiembre de 2020.

Se destaca la publicación de una tarjeta informativa con carácter secreto, elaborada el 2 de septiembre de 2020 bajo el nombre "Actividades Raymundo Ramos", en la que se da cuenta de las conversaciones que sostuvo el defensor de derechos humanos con periodistas, entre el 16 de agosto y el 26 de agosto de 2020; es decir, exactamente durante las fechas en que el análisis forense de Citizen Lab concluyó que el teléfono de Raymundo Ramos estaba infectado con *Pegasus*.

Además, fueron publicados documentos obtenidos a partir de la filtración realizada por el colectivo Guacamaya que revelan la estructura militar que se encuentra detrás del uso de *Pegasus*: el Centro Militar de Inteligencia (C.M.I.). La tarjeta informativa mencionada previamente fue elaborada por el C.M.I., dependencia que formaba parte de la Subjefatura de Inteligencia del Estado Mayor de la Defensa Nacional, el brazo operativo del Secretario de la Defensa Nacional. Otros documentos refieren que la misión y objetivo del C.M.I. consiste en "administrar y operar la infraestructura tecnológica del Sistema de Inteligencia Militar" y "aportar productos de inteligencia que se generen de la información obtenida en medios cerrados", es decir, a través

de la intervención de comunicaciones privadas, sin que las fuerzas armadas cuenten con facultades legales para dichas tareas.

En otro documento se observa que el C.M.I. es mencionado como el usuario final del "Sistema de Monitoreo Remoto de Información" que adquirió la SEDENA a través de Comercializadora Antsua, empresa designada con los derechos exclusivos para la venta de *Pegasus* al Ejército.

Adicionalmente, se demostró que la tarjeta informativa que da cuenta del espionaje ilegal con *Pegasus* a Raymundo Ramos fue elaborada y revisada por altos mandos militares, incluido el Jefe del Estado Mayor de la Defensa Nacional, el Subjefe de Inteligencia, el Director del C.M.I. y otras dos personas analistas en el C.M.I. y se comprobó que fue realizada para conocimiento del Secretario de la Defensa. Finalmente, se publicaron documentos que demuestran que el mismo día en que fue elaborado el documento, se llevó a cabo una reunión en la oficina del Secretario de la Defensa en la que el más alto mando militar se reunió con el Jefe del Estado Mayor, el Subjefe de Inteligencia y otros mandos militares para discutir como tema: "Nuevo Laredo, Tamaulipas".

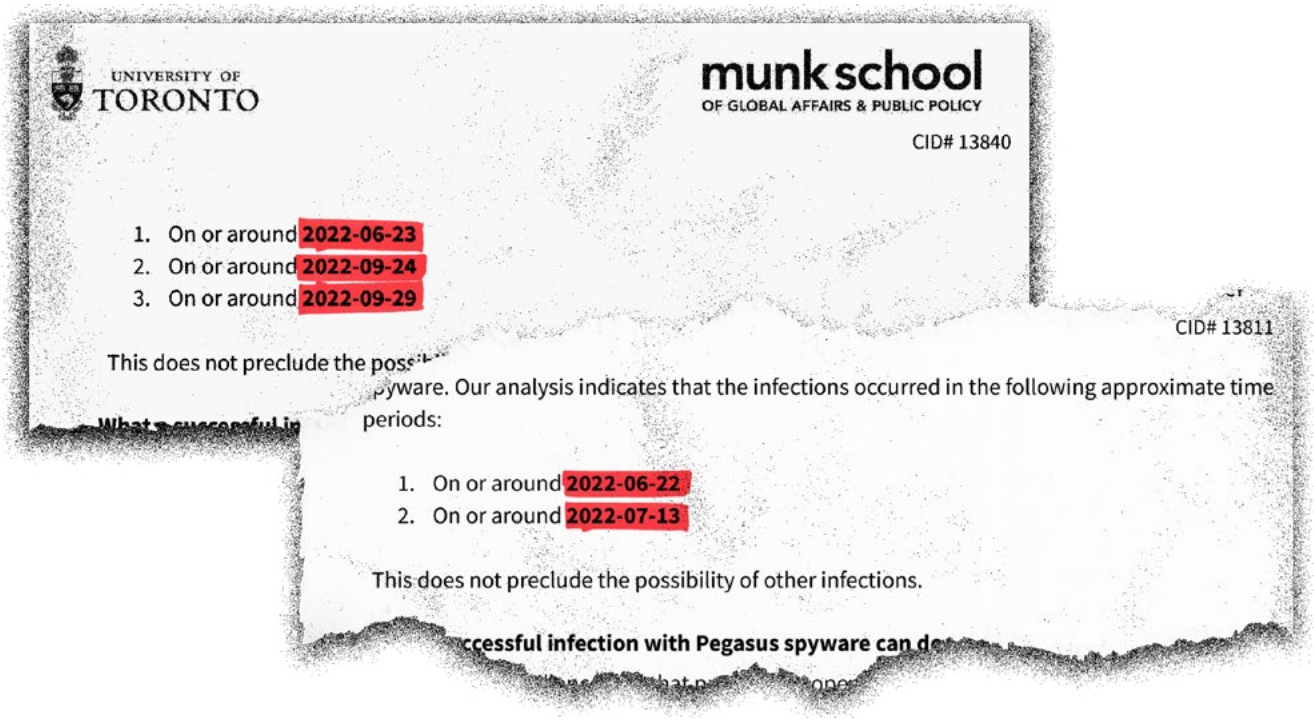
Cabe señalar que la SEDENA es una de las instituciones que no hizo públicos los contratos con NSO para la adquisición de *Pegasus* u otros sistemas de espionaje, como lo había prometido públicamente el titular del Ejecutivo. La información que se ha hecho pública a partir del hackeo realizado por el Colectivo Guacamaya da cuenta de las actividades de vigilancia y monitoreo que realiza la SEDENA a organizaciones civiles y personas defensoras de derechos humanos, activistas y periodistas, en uno de ellos incluye al Centro Prodh, junto con otras organizaciones de sociedad civil, en donde las mismas son catalogadas como "grupos de presión", por su trabajo de defensa de derechos humanos.

NUEVO ESPIONAJE CONTRA EL CENTRO PRODH

El 15 de diciembre de 2022, dos dispositivos móviles del Centro Prodh recibieron un correo electrónico proveniente de Apple y dirigido a su cuenta en iCloud, en el que la empresa notificó a las personas usuarias que sus dispositivos habrían sufrido una intromisión ilegal por "atacantes patrocinados por el Estado". Posteriormente, mediante dictamen de 17 de abril de 2023, Citizen Lab, confirmó que dichos dispositivos efectivamente fueron infectados mediante el *software Pegasus* en el año 2022 en al menos cinco ocasiones.

Los investigadores de Citizen Lab analizaron los dispositivos de Santiago Aguirre Espinosa, Director del Centro Prodh, y María Luisa Aguilar Rodríguez, coordinadora del Área Internacional, obteniendo resultados

positivos, lo que de acuerdo con el dictamen indica que los dispositivos examinados, fueron infectados con el *spyware Pegasus*, estableciendo que las infecciones se produjeron alrededor de junio, julio y septiembre de 2022 sin excluir la posibilidad de otras infecciones.



UNIVERSITY OF TORONTO

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

CID# 13840

1. On or around 2022-06-23
2. On or around 2022-09-24
3. On or around 2022-09-29

This does not preclude the poss

CID# 13811

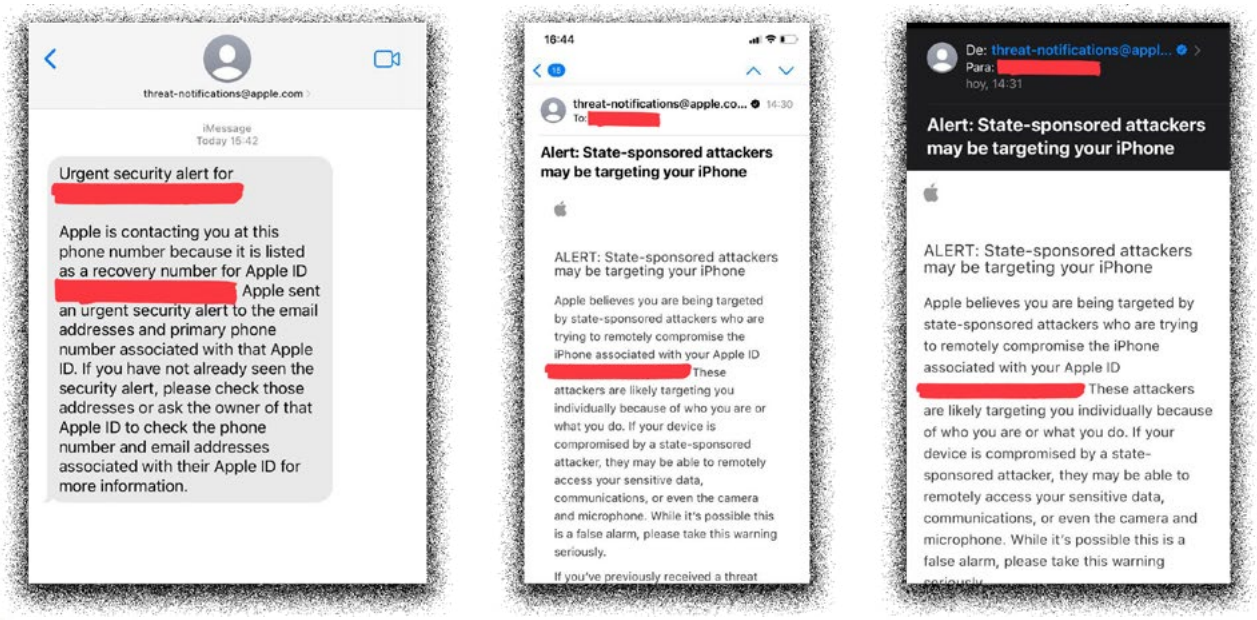
pyware. Our analysis indicates that the infections occurred in the following approximate time periods:

1. On or around 2022-06-22
2. On or around 2022-07-13

This does not preclude the possibility of other infections.

ccessful infection with Pegasus spyware can d

Extracto del análisis forense de Citizen Lab de la Universidad de Toronto donde se muestran las fechas de infección con Pegasus a los dispositivos de dos integrantes del Centro Prodh.



threat-notifications@apple.com

iMessage
Today 15:42

Urgent security alert for [redacted]

Apple is contacting you at this phone number because it is listed as a recovery number for Apple ID [redacted] Apple sent an urgent security alert to the email addresses and primary phone number associated with that Apple ID. If you have not already seen the security alert, please check those addresses or ask the owner of that Apple ID to check the phone number and email addresses associated with their Apple ID for more information.

16:44

threat-notifications@apple.co... 14:30
To: [redacted]

Alert: State-sponsored attackers may be targeting your iPhone

ALERT: State-sponsored attackers may be targeting your iPhone

Apple believes you are being targeted by state-sponsored attackers who are trying to remotely compromise the iPhone associated with your Apple ID [redacted] These attackers are likely targeting you individually because of who you are or what you do. If your device is compromised by a state-sponsored attacker, they may be able to remotely access your sensitive data, communications, or even the camera and microphone. While it's possible this is a false alarm, please take this warning seriously.

If you've previously received a threat

De: threat-notifications@appl...
Para: [redacted]
hoy, 14:31

Alert: State-sponsored attackers may be targeting your iPhone

ALERT: State-sponsored attackers may be targeting your iPhone

Apple believes you are being targeted by state-sponsored attackers who are trying to remotely compromise the iPhone associated with your Apple ID [redacted] These attackers are likely targeting you individually because of who you are or what you do. If your device is compromised by a state-sponsored attacker, they may be able to remotely access your sensitive data, communications, or even the camera and microphone. While it's possible this is a false alarm, please take this warning

Capturas de pantalla de las notificaciones enviadas por Apple a los dispositivos de dos integrantes del Centro Prodh.

Es importante señalar que en el caso del Director del Centro Prodh, ya había sido previamente objeto de ataques con *Pegasus* en el año 2016 y fue denunciante ante la FGR, firmando la denuncia de los hechos, compareciendo a ratificar y rendir entrevista, e incluso aceptando que la autoridad a cargo de la investigación requiriera e incorporara en la carpeta de investigación información personal como el registro de sus llamadas.

Es decir, a través de la infección a dicha persona, la misma organización de derechos humanos fue objeto de espionaje con *Pegasus* en dos administraciones distintas, lo cual muestra cómo la impunidad y la falta de medidas adecuadas, derivó en la repetición de los hechos de espionaje ilegal.

Las actividades realizadas por el Centro Prodh en momentos cercanos a la infección, se encuentran vinculadas a la constante denuncia que como organización de derechos humanos ha sostenido respecto al empoderamiento de las Fuerzas Armadas en tareas de seguridad pública sin controles adecuados, así como la exigencia de rendición de cuentas del Ejército en casos emblemáticos de violaciones a derechos humanos, como el caso Ayotzinapa, Tlatlaya, Guerra Sucia, el asesinato de sacerdotes jesuitas en Cerocahui, Chihuahua, entre otros.

A continuación, se señalan algunas de las fechas y actividades relevantes realizadas por el Centro Prodh en este contexto (centrándonos únicamente en el año en que ocurrieron las infecciones), mostrando cómo el trabajo que realiza el Centro Prodh se relaciona con la documentación, exigencia y denuncia por violaciones a derechos humanos.

Acción Global por Ayotzinapa. Familiares realizan cada mes una marcha para exigir verdad y justicia por sus 43 hijos desaparecidos. El Centro Prodh es una de las organizaciones que acompaña y representa a las familias.

EVENTO	FECHA
Elementos de inteligencia de SEDENA realizan nota sobre valoración del Aniversario del siniestro ocurrido en Pasta de Conchos, haciendo referencia a las organizaciones, como el Prodh, que acompaña a las víctimas, así como posible inviabilidad del rescate (documento obtenido por el Colectivo Guacamaya) hecho público en Proceso el 19 de febrero de 2023).	15/02/2022
Se presenta el Tercer Informe del GIEI, en el caso Ayotzinapa (el Centro Prodh es representante legal y acompaña a las familias, además de que fue quien gestionó ante la CIDH la creación del GIEI en 2014). En el Informe se destaca información de vigilancia militar a los estudiantes y posteriormente a las familias, así como presencia de elementos de la Marina mediante video de dron en el basurero de Cocula.	28/03/2022
Envío por parte de SEDENA de un documento de valoración de una entrevista otorgada por el Prodh en torno al caso de la ejecución extrajudicial de Ángel Yael Ignacio Rangel por parte de elementos de la Guardia Nacional. En el documento se refiere que las declaraciones del Director del Centro Prodh son “imprecisas” y que tienen el objetivo de “justificar el financiamiento de la organización” (Documento obtenido por el Colectivo Guacamaya).	14/05/2022
Homicidio de los sacerdotes jesuitas Joaquín Mora y Javier Campos en Cerocahui, Chihuahua. El Centro Prodh como organización fundada por la Compañía de Jesús, acompaña la denuncia y acciones en seguimiento.	20/06/2022
Evento en el Campo Militar No. 1 en el contexto del Mecanismo de Esclarecimiento de casos de la Guerra Sucia. En el evento participó Alicia de los Ríos, quien busca a su madre desaparecida en dicho contexto y es acompañada nacional e internacionalmente ante la CIDH por el Centro Prodh.	22/06/2022
Fecha aproximada de infección al Director del Centro Prodh.	22/06/2022

EVENTO	FECHA
Fecha aproximada de infección a la Coordinadora del Área Internacional del Centro Prodh.	23/06/2022
Audiencia pública con la Comisión de Derechos Humanos Tom Lantos del Congreso de EUA en la que participó el Prodh en la cual se hizo referencia al caso de los jesuitas asesinados en Cerocahui, el caso Ayotzinapa y el caso de la familia Barajas de Guanajuato.	23/06/2022
El Centro Prodh, junto con el representante de la Compañía de Jesús en México, acudió a una reunión en Chihuahua para abordar el caso de Cerocahui, con representantes del gobierno de dicha entidad, así como con representantes de seguridad, incluyendo de la SEDENA y Guardia Nacional.	24/06/2022
Centro Prodh señala en distintos espacios mediáticos, entre ellos, *Proceso* y de *Aristegui Noticias*, un análisis sobre el fracaso de la estrategia de seguridad y la profundización de la militarización, bajo la perspectiva de los derechos humanos.	27/06/2022
Se hizo pública información sobre 2 nuevas órdenes del Ejército para "abatir delincuentes" como la referida en caso Tlatlaya, caso acompañado por el Centro Prodh (en el contexto de aniversario de las ejecuciones ocurridas en 2014). También se publicó información sobre la destrucción de documentos del batallón de Tlatlaya, ocurrida en 2017.	30/06/2022
Fecha aproximada de infección al Director del Centro Prodh.	13/07/2022
Documento de inteligencia de la SEDENA en el que el área de inteligencia solicita hacer seguimiento a declaraciones de religiosos jesuitas en caso Cerocahui tras considerar declaraciones de algunos de ellos críticas al gobierno (Documento obtenido por el Colectivo Guacamaya).	15/07/2022

EVENTO	FECHA
Documento de inteligencia militar de la SEDENA cataloga al Centro Prodh como “grupo de presión”. (Documento obtenido por el Colectivo Guacamaya).	08/08/2022
Publicación del informe de la presidencia de COVAJ en el caso Ayotzinapa. El informe se presenta en reunión con AMLO en Palacio Nacional, con presencia de todo el gabinete de seguridad. El Centro Prodh acude como representante de las familias e integrante de la COVAJ. En dicho informe se vincula a la SEDENA con la operación de *Pegasus* para hacer seguimiento de diversas personas relacionadas al Caso Ayotzinapa y se publican documentos con transcripciones sobre las intervenciones en las que aparecen las siglas del C.M.I.	18/08/2022
Fecha del pliego de consignación en contra de militares y otras autoridades por el caso Ayotzinapa. El Centro Prodh como representante legal de las familias, forma parte como coadyuvante del ministerio público.	18/08/2022
Detención de Jesús Murillo Karam, titular de la PGR al inicio de la investigación del caso Ayotzinapa y posterior vinculación a proceso (24 de agosto) por desaparición forzada, tortura y obstrucción de la justicia. La detención ocurre mientras el Fiscal Especial para el caso no se encuentra presente en el país. El Centro Prodh como representante legal y coadyuvante, acude a las diversas audiencias.	19/08/2022
Anuncio de la FGR de 83 órdenes de aprehensión relacionadas con el caso Ayotzinapa (incluyendo 20 de militares). El Centro Prodh junto con las familias exige su cumplimiento y el adecuado avance de los procesos para el esclarecimiento del caso.	19/08/2022
Centro Prodh realiza distintos pronunciamientos y análisis en medios de comunicación (como el Juego de la Corte de Nexos) para condenar las iniciativas las modificaciones legislativas con las que se adscribiría la Guardia Nacional a la SEDENA.	01/09/2022

EVENTO	FECHA
Conferencia de prensa sobre ejecución de la menor de edad Heidi por elementos del Ejército en Tamaulipas, la conferencia es encabezada por Raymundo Ramos y se lleva a cabo en el Centro Prodh.	08/09/2022
FGR presenta documento mediante el cual solicita la cancelación de 21 órdenes de aprehensión en el caso Ayotzinapa, incluyendo las de varios militares. El Centro Prodh señala su preocupación ante presiones e injerencia del Ejército en la investigación.	13/09/2022
Luego que la CNDH publicara un comunicado para indicar que promovería acción de inconstitucionalidad ante la adscripción de la GN a Sedena, el Centro Prodh realiza pronunciamientos públicos para criticar esta decisión y señalar los riesgos de la creciente militarización.	14/09/2022
Detención del general de la SEDENA José Rodríguez Pérez por caso Ayotzinapa y dictado de auto de formal prisión (21 de septiembre). Se ejecutaron en total 4 órdenes de aprehensión en contra de militares y el resto fueron canceladas. El Centro Prodh se pronuncia exigiendo el adecuado avance de los procesos para el esclarecimiento del caso.	15/09/2022
Ante la discusión en el Senado de ampliar el plazo para que Fuerzas Armadas permanezcan en tareas de seguridad, Centro Prodh hizo distintos pronunciamientos públicos para criticar esta decisión y llamó al legislativo a no aprobar estas reformas y a abrir un debate profundo en estos temas.	21/09/2022
Protesta de normalistas y familiares de estudiantes desaparecidos de Ayotzinapa afuera del Campo Militar No. 1.	23/09/2022
Fecha aproximada de infección a la Coordinadora del Área Internacional del Centro Prodh.	24/09/2022

EVENTO	FECHA
Se publica en el diario Reforma la filtración de información del informe de COVAJ que se encontraba testada y se hace pública información sobre la cancelación de órdenes de aprehensión que habían sido solicitadas por FGR, incluyendo de militares.	24/09/2022
Octavo Aniversario de los hechos de Ayotzinapa). El Centro Prodh acompaña a las familias como sus representantes. Las familias son alojadas, como en cada visita que realizan a la CDMX, en las instalaciones del Centro Prodh.	26/09/2022
Se hace pública la renuncia del Fiscal Especial para el caso Ayotzinapa derivada de la intromisión en su investigación por parte del Fiscal General. El Centro Prodh expresa su preocupación.	27/09/2022
El diario Reforma publica en su primera plana chats de integrantes de Guerreros Unidos con elementos de Marina y SEDENA, mostrando la vinculación entre dicha institución y el crimen organizado.	27/09/2022
Fecha aproximada de infección a la Coordinadora del Área Internacional del Centro Prodh.	29/09/2022
Publicación del IV Informe del GIEI en donde se refieren a la cancelación de órdenes de aprehensión, la intromisión en la investigación, los vínculos del Ejército en Guerrero con crimen organizado, así como la necesidad de realizar la revisión de la veracidad de mensajes de texto incluidos en el informe de la COVAJ. El informe también refiere documentos en los que se menciona al C.M.I. y denuncia la negativa por parte de la SEDENA de entregar documentos del área de inteligencia militar. El Centro Prodh acompaña como representantes a las familias en la presentación.	29/09/2022

EVENTO	FECHA
Publicación periodística en *El País* en la que se retoma que está en duda la fidelidad de los mensajes que forman parte del informe de COVAJ y que están siendo revisados por el GIEI. El Prodh acompaña mensajes públicos con preocupación por el impacto en el esclarecimiento.	29/09/2022
Se revela el hackeo realizado a la SEDENA por el Colectivo Guacamaya.	29/09/2022
Luego de que el Senado continuara con la discusión para ampliar el plazo de permanencia de las Fuerzas Armadas en tareas de seguridad, publicamos una serie de imágenes con las conversaciones de Guerreros Unidos que aludían a la relación que mantenían con el Ejército. Estas conversaciones fueron dadas a conocer por el GIEI en el IV Informe por el caso Ayotzinapa.	4/10/2022

Agradecemos a la organización Data Cívica su apoyo y asesoría para la revisión de documentos provenientes del Colectivo Guacamaya.

Mujeres de Atenco arropan la lucha por la libertad de Keren Ordóñez, victima de tortura y discriminación en razón de género, acompañada por el Centro Prodh.

El trabajo del Centro Prodh en casos de violaciones a derechos humanos vinculados con el Ejército ha sido constante, denunciando los riesgos de la militarización ante diversas instancias internacionales como la CIDH (desde su primer visita al país en 1996) y la ONU (mediante informes de diferentes procedimientos especiales), instancias que han retomado los pronunciamientos e información aportada por el Centro Prodh al emitir informes y recomendaciones al Estado, respecto a la necesidad de establecer un modelo de seguridad civil y mayores controles al Ejército.

El Centro Prodh también ha acompañado y defendido legalmente a víctimas y sobrevivientes de graves violaciones a derechos humanos cometidas por las Fuerzas Armadas, incluyendo casos de tortura, tortura sexual, detenciones arbitrarias, ejecuciones extrajudiciales y desapariciones forzadas, tanto en el ámbito nacional como internacional. Lo anterior se suma a la emisión de informes y análisis que se han realizado constantemente respecto a reformas legales y la implementación de políticas que se han realizado para ampliar facultades del Ejército en tareas de seguridad pública.

En 2022, habitantes de Xochimilco y Azcapotzalco, acompañados por el Centro Prodh, presentaron quejas en contra de la construcción de cuarteles de la Guardia Nacional.

CONCLUSIONES

La repetición del espionaje al Centro Prodh, es decir, el ataque a la misma organización en dos gobiernos distintos resulta especialmente grave. Por un lado, reitera y profundiza las afectaciones a los derechos humanos de las personas espiadas, así como a la organización en su conjunto; más grave aún, evidencia el interés de quien lo comete de interferir en el legítimo trabajo de defensa de derechos humanos, acompañamiento a víctimas de graves violaciones a derechos humanos y exigencia de verdad y justicia, que ha mantenido de forma constante el Centro Prodh, independientemente de cambios de gobierno, detonando las mismas consecuencias.

La impunidad que ha prevalecido respecto a las denuncias de espionaje en contra de integrantes del Centro Prodh (entre otras personas) en el pasado, en gran medida posibilitó la reiteración de los hechos. La Fiscalía General de la República ha fallado en que los responsables del espionaje rindan cuentas por la adquisición y uso de *Pegasus*, mostrando la falta de voluntad y capacidad técnica para deslindar responsabilidad en uno de los casos con mayor cobertura internacional. Tampoco se ha tomado ninguna otra medida de no repetición como el emprendimiento de reformas legales, ni se ha cumplido a cabalidad con la exigencia de transparentar los contratos de adquisición de Pegasus.

El espionaje cometido por el Ejército a integrantes de una organización de derechos humanos como el Centro Prodh, en contextos de exigencia de verdad y justicia, así como de denuncia de la militarización, da cuenta de una institución militar en creciente empoderamiento y sin controles adecuados, resistente a rendir cuentas y que funciona bajo lógicas poco democráticas, sin subordinación al orden civil, lo que confirma las consecuencias para los derechos humanos y para la democracia de la profundización de la militarización que actualmente vivimos.

Centro Prodh
CENTRO DE DERECHOS HUMANOS
MIGUEL AGUSTÍN PRO JUÁREZ A.C.

R3D
Red en Defensa
de los Derechos Digitales

SOCIAL TIC

ARTICLE 19