# Informe conjunto sobre la situación de las personas defensoras de derechos humanos en las Américas: los casos de vigilancia electrónica ilegal

## I. Introducción

Las organizaciones que firman este documento forman parte del consorcio "Al Sur", un grupo organizado de la sociedad civil en América Latina que busca fortalecer los derechos humanos en el entorno digital. La razón principal de este documento es compartir información particular de la situación de las personas defensoras de derechos humanos en las Américas respecto al uso ilegal de tecnologías de vigilancia por parte de los Estados y empresas privadas sobre ellas, poniendo en riesgo sus derechos humanos, civiles y políticos.

Como veremos a lo largo del informe, estas tecnologías de vigilancia están siendo crecientemente usadas por los Estados en América Latina y el Caribe como forma de amedrentamiento, perfilamiento y vigilancia sobre defensores de derechos humanos por el simple hecho de realizar su labor, a veces incómoda y otras directamente confrontacional con las políticas de algunos Estados y de algunas empresas privadas. Vemos con preocupación cómo el uso de este tipo de tecnologías para estos fines se hace común, cómo los marcos legales y jurídicos muchas veces no están preparados para estos retos, y cómo los derechos humanos de defensores, pero también de sus comunidades afines se ven crecientemente afectados.

Así, este informe dará un panorama resumido, ejemplificando la situación en algunos países del continente, comentará sobre tendencias regionales y dará recomendaciones técnicas para hacer frente al escenario. Este documento ha sido hecho sobre la base de otros reportes de denuncia de la situación que “Al Sur” ha hecho, como “The acquisition and abuse of private surveillance technologies in Latin America” (2018),[1] hecho para colaborar en el llamado de presentaciones para el informe “The Surveillance Industry and Human Rights” coordinado por la Relatoría Especial de la ONU en la promoción y protección del derecho a la libertad de opinión y expresión; y el informe “Recomendaciones para la transparencia y anticorrupción en la adquisición y uso de tecnologías de vigilancia por parte de los Estados americanos” (2018),[2] hecho en el marco de la VII Cumbre de las Américas realizada en Perú.

Esperamos, de esta forma, que este documento sea un aporte para que la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH) y la Comisión

[1] Entrega de Organizaciones Latinoamericanas al Relator especial de la ONU en la promoción y protección del derecho a la libertad de opinión y expresión. 2019. https://www.tedic.org/la-adquisicion-y-el-abuso-de-tecnologias-de-vigilancia-en-america-latina-al-sur/

[2] Recomendaciones para la transparencia y anticorrupción en la adquisición y uso de tecnologías de vigilancia. 2018. https://adcdigital.org.ar/2018/04/26/recomendaciones-para-la-transparencia-y-anticorrupcion-en-la-adquisicion-y-uso-de-tecnologias-de-vigilancia/

Interamericana de Derechos Humanos (CIDH),[3] y que obtengan así un panorama bien documentado de cómo las tecnologías son hoy usadas ilegalmente en el continente para impedir la labor de las personas defensoras de derechos humanos.

## II. Algunos casos emblemáticos en la región

Ha habido diversos casos bien documentados de abuso estatal de tecnologías de vigilancia privada, sin aparente justificación legal o autorización judicial, contra activistas o grupos de la sociedad civil particularmente críticos o inconvenientes para los intereses de las personas en el poder.

Por ejemplo, en **México**, un malware llamado "Pegasus", que es extremadamente sofisticado e intrusivo y comercializado por la compañía israelí NSO Group, se ha utilizado para atacar a periodistas y defensores de derechos humanos, abogados, activistas de salud pública y anticorrupción, así como el cuerpo internacional de expertos independientes designados para investigar la desaparición de los 43 estudiantes de Ayotzinapa en 2014.[4]

En junio de 2017, la gravedad del caso hizo que diversos Relatores Especiales de la ONU pidieran a México que estableciera una investigación independiente e imparcial sobre el despliegue de “Pegasus”.[5] Ésta también ha sido una demanda reiterada de las víctimas. Sin embargo, hasta la fecha, los gobiernos salientes y entrantes no han reconocido el establecimiento de garantías de tal investigación y el proceso penal en curso ha mostrado poco

---

[3] ACNUDH y CIDH piden contribuciones para informe sobre la situación de las personas defensoras de derechos humanos en las Américas http://acnudh.org/acnudh-y-cidh-piden-contribuciones-para-informe-sobre-la-situacion-de-las-personas-defensoras-de-derechos-humanos-en-las-americas-fecha-limite-10-de-junio-de-2019/

[4] Artículo 19, Citizen Lab, R3D: Red en Defensa de los Derechos Digitales, SocialTIC. (junio 2017) Gobierno Espía: Vigilancia sistemática a periodistas y defensores de derechos humanos en México. Disponible en: https://r3d.mx/gobiernoespia/ ; R3D. Destapa la Vigilancia: promotores del impuesto al refresco, espiados con malware gubernamental. Disponible en: https://r3d.mx/2017/02/11/destapa-lavigilancia-promotores-del-impuesto-al-refresco-espiados-con-malware-gubernamental/ ; 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=fbshare&_r=0 ;Ahmed, Azam. Perlroth, Nicole. (June 19, 2017) Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families. The New York Times. Disponible en: https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html ; 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-penanieto-corrupcion/ ; Ahmed, Azam. (July 10, 2017) Spyware in Mexico Targeted Investigators Seeking Students. The New York Times. Disponible en: https://www.nytimes.com/2017/07/10/world/americas/mexico-missing-students-pegasus-spyware.html

[5] United Nations Human Rights: Office Of The High Commissioner (July 21, 2017) Mexico: UN experts call for an independent and impartial investigation into use of spyware against rights defenders and journalists https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21892

progreso; sin mencionar que no se han instalado procedimientos para investigar y procesar las claras indicaciones de corrupción detrás de la adquisición de este malware.

En la misma línea, en **Panamá**, se ha establecido un procedimiento penal contra el ex Presidente Ricardo Martinelli donde se le atribuye los delitos de inviolabilidad del secreto y del derecho a la intimidad al utilizar "Pegasus", un sistema de escuchas y espionaje telefónico, para interceptar comunicaciones y practicar vigilancia sin autorización judicial contra aproximadamente 150 personas, incluidos periodistas, empresarios, líderes de la sociedad civil, miembros de la oposición e incluso de su propio partido.[6] Se ha estimado que entre 2009 y 2014, el gobierno de Martinelli adquirió tecnologías de vigilancia por 13,5 millones de dólares de las compañías M.L.M. Protección Ltd. y Grupo NSO, los que a la fecha se encuentran desaparecidos.[7]

Concluido su periodo presidencial, el exmandatario viajó a Ciudad de Guatemala donde fue juramentado como diputado en el Parlamento Centroamericano (PARLACEN) revistiéndose de inmunidad y se autoexilió en los Estados Unidos alegando persecución política orquestada por el actual gobierno en su contra. El 17 de junio de 2017 fue detenido en atención al pedido de extradición que mantenía Panamá y posteriormente enviado a Panamá el 11 de junio de 2018 por el caso de escuchas telefónicas[8]. Un testigo protegido afirma que mientras laboraba en el Consejo de Seguridad Nacional de Panamá, organismo encargado de las supuestas escuchas telefónicas, su jefe directo afirmó en reiteradas ocasiones que las órdenes de intervenir ilegalmente distintos teléfonos venían directamente del ex presidente Martinelli, quien se encuentra con medida cautelar de detención domiciliaria, con la confiscación de sus pasaportes y la prohibición de hablar del proceso que se lleva en su contra en redes sociales[9].

En tanto en **Chile**, una de las situaciones más relevantes en el contexto de este informe es, sin lugar a duda, el uso de tecnologías de vigilancia en contra de las personas defensoras de las comunidades indígenas mapuche. Con motivo del Examen Periódico Universal (EPU) de Naciones Unidas que Chile se sometió a principios del 2019, Derechos Digitales destacó al respecto cómo en el país "se restringen ilegítimamente los derechos civiles y políticos del pueblo Mapuche, al intentar interceptar comunicaciones privadas de sus representantes, vulnerando no solo su derecho a la privacidad, sino además ejerciendo nuevas formas de

[6] Bonífaz, R and Delgado-Ron, A. (January 31, 2018) Verified cases of unlawful use of surveillance software by Latin American Governments 2015-2016, PUCE Magazine, ISSN:2528-8156, p. 315-333
[7] Acento (June 13, 2017) Cronología del caso de escuchas en Panamá por el que detienen a Ricardo Martinelli en EEUU. https://acento.com.do/2017/actualidad/8465768-cronologiadel-caso-escuchas-panama-detienen-ricardomartinelli-eeuu/
[8] Ricardo Martinelli es detenido en Miami. La Prensa. 12 de junio 2017 https://www.prensa.com/judiciales/Ricardo-Martinelli-detenido-Miami_0_4778522157.html
[9] Testigo reitera que Martinelli daba las órdenes. La Prensa. 14 de junio 2019. https://impresa.prensa.com/panorama/Testigo-reitera-Martinelli-daba-ordenes_0_5326717362.html

violencia institucional a través del uso de la tecnología, intentando criminalizarlos a través de la implantación de pruebas falsas en sus teléfonos celulares".[10]

Se trata de la llamada "Operación Huracán", donde el 2017 Carabineros implantó pruebas falsas a los celulares de ocho comuneros mapuche por su supuesta participación en una serie de atentados incendiarios.[11] El ahora conocido "Caso Huracán" está siendo investigado por la fiscalía y se ha convertido en un verdadero escándalo político en tanto, tal como reconoce Derechos Digitales, también ha desentrañado "la preocupante acción de agentes de la policía y de servicios de inteligencia que han vigilado y monitoreado a activistas políticos, periodistas y medios de comunicaciones, tanto en espacios físicos como digitales, restringiendo la libertad de expresión y su habilidad de organizarse políticamente".[12]

Según un informe de la misma ONG,[13] el fracaso de la "Operación Huracán" ha permitido conocer distintos tipos de vigilancia ilegal al pueblo mapuche y otros activistas, como:

a) Escuchas telefónicas ilegales: En el marco de las actividades realizadas por la Unidad de Inteligencia Operativa Especializada (UIOE) de La Araucanía, que lideraba la "Operación Huracán", entre el año 2016 y el 2018 intervino un número indeterminado de teléfonos, que se estima se encontraría en algún punto entre los 200 y los 1000. El informe dice que "los teléfonos son de dirigentes mapuches, pero también de políticos, jueces, fiscales, abogados, actores y periodistas; la mayoría sin relación con la causa mapuche".
b) Acceso a metadatos telefónicos: **"**La investigación periodística de Nicolás Sepúlveda establece que la UIOE tenía acceso a Vigía, el software utilizado por todas las compañías de telecomunicaciones en Chile para administrar el registro de los metadatos de las comunicaciones, incluyendo los datos de llamadas recibidas, realizadas, la duración de estas y la antena que se utilizó para concretarlas. Pero no solo eso, sino que además el software conservaría también los mensajes de texto de un número telefónico".
c) Phishing: Una de las técnicas utilizadas por la UIOE para la diseminación de software malicioso era la creación de falsos perfiles en redes sociales, particularmente Facebook, con el fin de engañar a los blancos y enviar un *keylogger* para obtener sus credenciales de acceso a distintas plataformas. Otra de las técnicas de phishing utilizadas era la

[10] Chile bajo Examen Periódico Universal de obligaciones de DDHH: El futuro es ahora. 20 de diciembre 2018. https://www.derechosdigitales.org/12696/chile-bajo-examen-periodico-universal-de-obligaciones-de-ddhh-el-futuro-es-ahora/
[11] Sentirnos observados: ¿Qué sabemos sobre la vigilancia estatal en Chile?. 13 de septiembre 2018. https://www.derechosdigitales.org/12425/sentirnos-observados-que-sabemos-sobre-la-vigilancia-estatal-en-chile/
[12] Chile bajo Examen Periódico Universal de obligaciones de DDHH: El futuro es ahora. 20 de diciembre 2018. https://www.derechosdigitales.org/12696/chile-bajo-examen-periodico-universal-de-obligaciones-de-ddhh-el-futuro-es-ahora/
[13] Tecnología y vigilancia en la Operación Huracán: una revisión del trabajo periodístico realizado en torno al caso. Septiembre 2018. https://www.derechosdigitales.org/wp-content/uploads/tecnologia-y-vigilancia-en-huracan.pdf

preparación de correos electrónicos con programas maliciosos disfrazados como software inofensivo.

A todo lo anterior se suma que la Policía de Investigaciones (PDI) había adquirido el malware “Phantom”, de la firma italiana Hacking Team, con el propósito de "obtener información para la cual no se otorgaría acceso mediante una orden judicial".[14]

Relacionado con los defensores del pueblo mapuche, en **Argentina** la Agencia Federal de Inteligencia (AFI) llevó adelante una investigación ilegal y paralela sobre la población mapuche de Chubut desde el año 2015, que incluyó la individualización y seguimiento de unas 30 personas, entre periodistas, docentes, activistas, funcionarios y hasta un concejal del departamento de Cushamen. Esta situación fue denunciada por primera vez en una audiencia realizada el 28 de agosto de 2015 -en la causa por la presunta usurpación de tierras-, instruida por el juez de Garantías Martín Zacchino.[15] En su visita del 2019 al país, el relator especial sobre el derecho a la privacidad de la ONU, Joseph Cannataci, expresó preocupación por esta situación y subrayó que se trata de una actividad prohibida por la ley y dirigida a una comunidad vulnerable, y destacó la actitud de los agentes de policía y los funcionarios del sistema de justicia, quienes “aceptan el producto de la vigilancia”.[16]

Resulta particularmente preocupante, en el caso mapuche, que los gobiernos de **Chile** y **Argentina** compartieran información falsa obtenida por supuesto espionaje electrónico para criminalizar a sus líderes, en lo que se denominó “Operación Andes”, que buscaba desarticular un presunto tráfico de armas desde Argentina hacia la Coordinadora Arauco Malleco en Chile.[17]

En tanto en **Brasil**, desde 2005 hasta 2015, la Oficina de Seguridad Institucional de Brasil (GSI) y la Agencia de Inteligencia Brasileña (ABIN) administraron una base de datos llamada GEO-PR.[18] Teóricamente constituida con el único propósito de proteger territorios indígenas, tierras de pequeños agricultores y el medio ambiente a través de los datos recopilados por los organismos públicos, la base de datos también permitió el seguimiento de ONGs y de movilizaciones, huelgas y manifestaciones que tuvieron lugar en país. El programa se reanudó a lo largo de 2015, pero la base de datos se donó a la Agencia Brasileña de Inteligencia. Bajo el gobierno de Bolsonaro, todas estas herramientas y permisos tienden a ser aún más

---

[14] Garay, Vladimir. (September, 28 2017) Poco y nada (o cuánto sabemos realmente sobre cómo nos vigilan). Derechos Digitales. https://www.derechosdigitales.org/11446/poco-y-nada-ocuantosabemos-realmente-sobre-como-nos-vigilan/

[15] Desde 2015 la AFI realiza inteligencia ilegal en la zona mapuche de Chubut. 12 de agosto 2017. https://www.tiempoar.com.ar/nota/desde-2015-la-afi-realiza-inteligencia-ilegal-en-la-zona-mapuche-de-chubut

[16] Naciones Unidas cuestionó el sistema de escuchas telefónicas vigente. 5 de junio 2019. https://www.pagina12.com.ar/198422-naciones-unidas-cuestiono-el-sistema-de-escuchas-telefonicas

[17] “Operación Andes”: el otro plan de Inteligencia que se vino abajo con el “Huracán”. 19 de febrero 2018. https://ciperchile.cl/2018/02/19/operacion-andes-el-otro-plan-de-inteligencia-que-se-vino-abajo-con-el-huracan/

[18] Figueiredo, Lucas. (December, 2016). O Grande Irmão: Abin tem mega-banco de dados sobre movimentos sociais. Intercept: https://theintercept.com/2016/12/05/abin-temmegabanco-de-dados-sobre-movimentos-sociais/

amenazantes, ya que el propio presidente prometió "terminar con el activismo en Brasil". De hecho, una de estas primeras acciones fue una orden ejecutiva que ordenaba a la oficina del Secretario de Gobierno “supervisar, coordinar, monitorear y acompañar las actividades y acciones de organizaciones internacionales y organizaciones no gubernamentales en el territorio nacional”.[19]

En **Colombia** las personas que trabajan en la defensa de derechos humanos y líderes sociales han sido víctimas de numerosos ataques físicos en los últimos años. De acuerdo con cifras de la ONG Somos Defensores, en el 2018 se registraron 155 asesinatos, lo que representa un aumento de más del 40% respecto al año anterior. Asimismo, de los casos priorizados por la Fiscalía General de la Nación, sólo se ha llego a la condena en menos del 9 %.[20] Esta situación de vulnerabilidad, ampliamente conocida por el país y debatida en distintos foros, marca el contexto en el que realizan su trabajo las personas que promueven los derechos humanos en este país.

Sin embargo, hasta ahora, no hay casos recientes en los que se haya llegado a condenas por hechos que involucren el uso de tecnologías de vigilancia o amenazas digitales en contra de personas defensoras de derechos humanos. Son frecuentes los casos en que estas personas han sido víctimas de amenazas por medios digitales y de robos de sus dispositivos. La ausencia de indicadores y protocolos que permitan hacer seguimiento a estos incidentes es un factor que contribuye a la ausencia de información sobre estas situaciones y sus consecuencias.

Finalmente, los defensores de derechos humanos y líderes sociales están en situación de vulnerabilidad en materia de seguridad digital. El país tiene mapeado y conoce los datos de los delitos financieros realizados por medios digitales, pero los problemas de periodistas, defensores de derechos humanos, líderes sociales u organizaciones de la sociedad civil no están documentados, no hay organizaciones, ni protocolos que los identifiquen, sigan y monitoreen.

En síntesis, el trabajo de defensa de derechos humanos y el de líderes sociales en Colombia se realiza en un contexto altamente peligroso, como evidencia el aumento constante de asesinatos de personas con estos perfiles. Aunque no hay casos recientes de condenas ni por política de Estado ni por delitos relacionados con el abuso de herramientas de vigilancia digital en contra de defensores de derechos humanos, es claro que, en primer lugar, el Estado colombiano cuenta con herramientas de vigilancia de las comunicaciones que van desde la interceptación hasta el acceso a dispositivos electrónicos. Segundo, no existen controles adecuados para el uso de estas herramientas. Tercero, hay casos de abuso por parte de antiguos miembros de organizaciones del Estado con acceso a estas herramientas. Cuarto, no hay un sistema y unas prácticas de monitoreo de agresiones digitales en la Fiscalía General de

[19] Presidência da República do Brasil. Medida Provisória nº 870, de 1º de janeiro de 2019. http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Mpv/mpv870.htm
[20] Somos Defensores, (abril de 2019). “La naranja mecánica. Informe Anual 2018”. Disponible en: https://somosdefensores.org/2019/04/23/la-naranja-mecanica/

la Nación, ni de entidades encargadas de las políticas de seguridad digital lo que dificulta hacer seguimiento a este tipo de casos.

## III. Tendencias regionales

### *A) La falta de transparencia detrás de la adquisición de tecnologías de vigilancia facilita el uso ilegal de éstas para perseguir personas defensoras de derechos humanos*

La mayoría de las tecnologías de vigilancia desarrolladas por las empresas privadas han sido negociadas y adquiridas por los Estados latinoamericanos bajo procedimientos opacos e irregulares. Existe una falta general de transparencia con respecto a estos procedimientos bajo el pretexto de la "seguridad nacional", por lo que la mayor parte de la información relacionada con estas adquisiciones ha sido publicada por denunciantes ("*whistleblowers*"), e investigaciones hechas por los medios de comunicación y la sociedad civil.

Por ejemplo, en el caso de **México** y su adquisición del malware "Pegasus", se reveló que la adquisición se realizó a través de una empresa intermediaria que no tenía un historial previo de comercialización de herramientas de vigilancia y que fue fundada por un ex empleado de la Fiscalía General. Además, se ha revelado que la dirección registrada de la empresa no corresponde a ninguna oficina real de la empresa y las personas registradas como SUS fundadores afirman no tener conocimiento de las actividades de la misma, lo que sugiere que sólo actuaron como fachadas.[21]

En el caso de **Chile**, por ejemplo, se supo que el proceso de compra del programa espía Oxygen Forensic por parte de la Unidad de Inteligencia Operativa Especializada de Carabineros de La Araucanía (y que fue utilizado para implantar pruebas falsas a los comuneros mapuche), se hizo a través de un intermediario que no figura en el listado oficial de Chile Proveedores (la empresa XmartLab), y que su compra no cumplió estándares legales: Carabineros pagó con dinero en efectivo sacado de los "gastos reservados" de la institución, lo que luego fue ocultado por el mismo ex general de Carabineros, Gustavo Villalobos, a la Contraloría General de la República, "probablemente en un intento por no dejar rastros de esas operaciones de inteligencia que desembocaron en la Operación Huracán".[22]

En el caso de **Panamá,** el Consejo de Seguridad Nacional estableció una relación comercial con la empresa israelí NSO Contract Materials, en la que se incluía el sistema Pegasus. A diferencia de la adquisición efectuada en 2010 a la empresa M.L.M. Protection, a quien se le compró un sistema para infiltrar ciertas computadoras, en esta ocasión, Panamá no produjo ninguna documentación de pago por este sistema. Dicho equipo se adquirió a través de la

[21] Olmos, Raul. (20 Febrero 2017) Subordinado de Murillo Karam, ligado a grupo empresarial que vendió Pegasus a la PGR. Mexicanos Contra la Corrupción y la Impunidad. https://contralacorrupcion.mx/pegasus-pgr/

[22] Bruno Villalobos ocultó a Contraloría la compra de software de Operación Huracán. 18 de marzo 2019.https://interferencia.cl/articulos/bruno-villalobos-oculto-contraloria-la-compra-de-software-de-operacion-huracan

sociedad Caribbean Holding Services Ltd, y no a través del Estado por lo que no existe documentación de la Contraloría General de la República cónsona con las leyes de contratación pública.[23]

En el caso de **Colombia,** fue gracias a la filtración de Hacking Team que se supo que la Dirección Nacional de la Policía (DIPON) había adquirido el software de control remoto *Galileo* a través de la empresa Robotec en 2013. Un nuevo contrato para adquirir de nuevo este software se estaba negociando a través de la empresa israelí NICE en el momento de la filtración en 2015.[24] No hay casos que comprueben su utilización, pero su existencia y la ausencia de controles efectivos para vigilar su utilización, generan preocupaciones frente, por un lado, a la llegada de gobiernos que bajo políticas regresivas en derechos humanos, decidan acudir a estas herramientas en detrimento de las personas defensoras de derechos humanos, o por otro, a funcionarios corruptos que las usen indebidamente. A esto se suma la inseguridad jurídica que existe para el uso de estas herramientas de hackeo por el Estado.[25]

*B) El preocupante uso de tecnologías de vigilancia por parte de empresas privadas en contra personas defensoras de derechos humanos.*

Es importante mencionar que las empresas privadas también están implementando sistemas de tecnologías de vigilancia contra personas defensoras de derechos humanos.

En **Brasil**, la empresa Vale S.A. es la presunta responsable de vigilar a defensores de la tierra y activistas ambientales, así como a los periodistas y a sus propios trabajadores, para evitar denuncias de varias violaciones de derechos humanos e impacto socioambiental que se producen en sus negocios.[26]

El caso se repite en otras empresas ubicadas en Brasil, como Anglo American, una compañía minera acusada de vigilar y amenazar a ciudadanos de Conceição do Mato Dentro,[27] donde la empresa está siendo expuesta por líderes comunitarios que critican la construcción de una

[23] Perito describe el equipo Pegasus y las diligencias realizadas. 9 de abril del 2019. http://laestrella.com.pa/panama/nacional/perito-describe-equipo-pegasus-diligencias-realizadas/24115531
[24] Digital Rights, “En Colombia PUMA no es como lo pintan”, 24 agosto 2015), disponible en: https://www.digitalrightslac.net/es/en-colombia-el-puma-no-es-como-lo-pintan/
[25] Fundación Karisma, “Cuando el Estado Hackea” (Diciembre de 2015), disponible en: https://karisma.org.co/cuando-el-estado-hackea-3/
[26] Pozzebom, Elina Rodrigues. (October, 2013). Vale espiona líderes e se infiltra em movimentos sociais, diz ex-funcionário. Senado Noticias. https://www12.senado.leg.br/noticias/materias/2013/10/24/vale-espiona-lideres-e-se-infiltra-emmovimentos-sociais-diz-ex-funcionario
[27] Sant'anna, Daniel. Maciel, Alice. (March, 2018). AGRESSÕES, VIGILÂNCIA, DESEMPREGO, PERSEGUIÇÃO E ISOLAMENTO: COMO VIVEM OS MORADORES QUE ENFRENTAM A GIGANTE DA MINERAÇÃO. Intercept Brasil. https://theintercept.com/2018/03/27/ameacas-moradores-mineracao-anglo-american/

represa gigante.[28] Es más, parte de estos ciudadanos tuvieron que solicitar ser parte de un programa nacional que protege a los defensores de los derechos humanos.[29]

En **Colombia**, con el reciente "Caso Avianca"[30] se ha conocido de las escuchas ilegales de las comunicaciones de miembros del sindicato de pilotos de la aerolínea Avianca por parte de organizaciones criminales privadas que obtuvieron acceso a las tecnologías de interceptación del Estado con ayuda de miembros actualmente en función de la propia Fiscalía General de la Nación y miembros en retiro del Ejército Nacional. La investigación penal se encuentra todavía en curso.

*C) La impunidad y la falta general de responsabilidad con respecto al abuso de las tecnologías de vigilancia sobre las personas defensoras de derechos humanos.*

A pesar de la gravedad de los casos de abuso contra los defensores de derechos humanos que se han mencionado, la mayoría de estos no se han investigado ni procesado adecuadamente; aún más importante, existe una falta general de responsabilidad por la adquisición irregular de tecnología de vigilancia y el uso abusivo de dichas herramientas contra la sociedad civil, incluidos periodistas y personas defensoras de derechos humanos.

Por ejemplo, prevalece la impunidad con respecto al abuso del malware "Pegasus" en **México** contra varios periodistas, personas defensoras de derechos humanos y activistas. Un factor importante para esta situación es el hecho de que el principal sospechoso de estar detrás de los ataques es la misma institución a cargo de la investigación criminal oficial. En este sentido, un obstáculo importante para la rendición de cuentas ha sido la falta de independencia legal y/o política por parte de las autoridades a cargo de investigar los casos de abuso.

La falta de regulaciones y protocolos sobre el uso de sofisticadas herramientas de vigilancia como el malware "Pegasus" también ha creado obstáculos para la responsabilidad de las instituciones que usan estas tecnologías. Por ejemplo, en **México**, la Procuraduría General de la República ha declarado que no tiene un registro de las personas que han sido atacadas con este malware y ha negado la existencia de registros o cualquier forma de auditar el uso de estas herramientas.

Asimismo, no obstante, la empresa NSO Group ha declarado públicamente que cuando se denuncian casos de abuso de sus productos, ellos llevan a cabo una investigación interna y suspenden la relación con el cliente abusivo, se ha documentado que los ataques en México

[28] Ferraz, Lucas. (January, 2018). Anglo American quer barragem quatro vezes maior que a de Fundão, que rompeu em Mariana: https://apublica.org/2018/01/a-sombra-datragedia-de-mariana-video/
[29] Ministry of Human Rights of Brazil. Programa de Proteção aos Defensores de Direitos Humanos. https://www.mdh.gov.br/navegue-por-temas/programas-de-protecao/ppddh-1/sobre-oppddh
[30] El Tiempo, "La Fiscalía va a oír a Efromovich por las chuzadas del Sindicato", 1 junio 2019), disponibe en: https://www.eltiempo.com/justicia/investigacion/fiscalia-va-a-oir-a-efromovich-por-caso-de-chuzadas-al-sindicato-370090

ocurrieron incluso meses después de que los casos se habían denunciado públicamente. Además, a pesar de haber sido solicitados para cooperar con la investigación criminal oficial, la empresa no prestó ningún tipo de asistencia a la investigación oficial.

Además, los fiscales carecen de los conocimientos, experiencia y / o recursos para llevar a cabo investigaciones sobre presuntos abusos de las tecnologías de vigilancia. En algunas ocasiones, como en el caso de México, a los fiscales se les niega el acceso a información crucial con el pretexto de seguridad nacional, lo que representa un serio obstáculo para el acceso a la justicia.

En **Colombia** existen un sinnúmero de investigaciones penales por las amenazas y muertes dirigidas en contra de personas defensoras de derechos humanos, pero en su gran mayoría se trata de casos en los que la Fiscalía General de la Nación no ha establecido[31] aún responsables.[32] Dicha entidad llega incluso a barajar la opción de que en algunos casos se trata de auto amenazas,[33] pero lo cierto es que se trata de investigaciones que no avanzan y las particularidades que pueden presentar los elementos digitales no se reconocen.

También se conocen casos de empleo ilegal de las tecnologías de vigilancia del Estado colombiano por parte de funcionarios corruptos. Así, integrantes de las Fuerzas Armadas en función o en retiro, miembros de la Fiscalía General de la Nación han realizado escuchas ilegales en contra de miembros de las Altas Cortes,[34] de periodistas, sindicalistas, entre otros. Esta práctica, que se configura en medio de hechos de corrupción, se ha convertido en un fantasma[35] que frecuentemente amenaza la privacidad e intimidad de diversos actores sociales. Creemos que la falta de información para corroborar o no sospechas se debe igualmente a la poca transparencia que existe por parte del Estado en el uso de estas tecnologías. Esto no permite controles efectivos, pues los que existen no operan, como sucede con la comisión del congreso colombiano para seguimiento de la ley de inteligencia que no ha entrado en funcionamiento.[36]

---

[31] El Espectador, “El fantasma detrás de las águilas negras” (12 sept. 2018), disponible en: https://www.elespectador.com/colombia2020/pais/el-fantasma-detras-de-las-aguilas-negras-articulo-857135

[32] Fundación Ideas para la Paz, “Agresiones y homicidios de líderes sociales”, (s.f), disponible en: http://ideaspaz.org/media/website/infografia-lideres.pdf

[33] Pacifista, “Es absurdo que digan que me autoamenacé: jefe de prensa de Petro”, (22 abril de 2019), disponible en: https://pacifista.tv/notas/es-absurdo-que-digan-que-me-autoamenace-jefe-de-prensa-de-petro/ https://www.bbc.com/mundo/noticias-america-latina-39583477

[34] El País, “Qué se sabe de las chuzadas a magistrados de la Corte constitucional” (3 mayo 2019), disponible en: https://www.elpais.com.co/colombia/que-se-sabe-de-las-chuzadas-a-magistrados-de-la-corte-constitucional.html

[35] El Espectador, “Reaparece el “fantasma” de las chuzadas”, (7 mayo 2019), disponible en: https://www.elespectador.com/opinion/editorial/reaparece-el-fantasma-de-las-chuzadas-articulo-854083

[36] El Espectador “Operaciones de inteligencia de FF.MM sin control ni vigilancia”, (5 junio 2015), disponible en: https://www.elespectador.com/noticias/politica/operaciones-de-inteligencia-de-ffmm-sin-control-y-sin-v-articulo-564565

## IV. Recomendaciones generales

*A) Fortalecimiento de la protección de los derechos humanos tanto en línea como en el mundo físico de las personas defensoras de derechos humanos*

Los estados deben garantizar y promover el derecho a la privacidad en línea y en el mundo físico de las personas defensoras, cumpliendo las obligaciones internacionales de nuestros estados en materia de derechos humanos. En esta misma línea, se debe garantizar y promover el derecho a la libertad de expresión, y la libertad de asociación y reunión pacífica, tanto en línea como en el mundo físico, cumpliendo con las obligaciones internacionales de nuestros estados en materia de derechos humanos.

Específicamente, se debe proteger el ejercicio de los derechos humanos en el entorno en línea de los periodistas y defensores de derechos humanos, permitiendo a la sociedad beneficiarse de su trabajo.

*B) Implementar el marco legislativo apropiado para regular e imponer límites sobre el uso de la tecnología de vigilancia, así como formas de transparencia y rendición de cuentas.*

En este sentido, se necesita desarrollar y promover nuevas regulaciones sobre tecnologías de vigilancia que cumplan los principios de legalidad, necesidad y proporcionalidad, sin ninguna forma de discriminación contra grupos específicos, particularmente pueblos indígenas y personas defensoras de derechos humanos.

Nuestros estados deben promover la rendición de cuentas de las policías y las agencias de inteligencia que realizan vigilancia física y de las comunicaciones, así como también monitoreo de actividades políticas en redes sociales, a través de políticas y marcos legales actualizados, así como garantizar la existencia de organismos de supervisión independientes e imparciales, dotados de los poderes necesarios para auditar, investigar y procesar eficazmente cualquier abuso en el uso de tecnologías de vigilancia por parte de actores estatales, lo que incluye tener acceso absoluto a cualquier información, instalación o equipo necesario para llevar a cabo sus funciones. Debido al preocupante panorama que hemos visto en este informe, es urgente promover medidas efectivas de transparencia respecto a adquisición estatal de tecnologías de vigilancia y el modo en que éstas se utilizan, así como medidas efectivas de supervisión civil respecto a las actividades de vigilancia por parte de agentes estatales.

Así, un marco legislativo adecuado debe establecer las salvaguardas necesarias contra el abuso, incluyendo:

- Regulación específica sobre el uso de herramientas de vigilancia que incorpore los principios de necesidad y proporcionalidad.
- Autorizaciones judiciales independientes y mecanismos de supervisión.
- Regulaciones que aseguran que el uso de la tecnología de vigilancia privada sea auditable por los organismos de supervisión.

- Transparencia respecto a las capacidades de vigilancia general del Estado e información significativa sobre el alcance y la extensión del uso de la tecnología de vigilancia privada.
- Asegurarse de que las personas que son objeto de vigilancia por tecnologías sean eventualmente notificadas y tengan acceso a compensaciones.

*C) Garantizar el apego a los derechos humanos de las empresas privadas que proveen tecnologías de vigilancia o que las usan sobre las personas defensoras de derechos humanos*

En el caso de las empresas productoras de tecnologías de vigilancia, deben evitar causar o contribuir a impactos adversos sobre los derechos humanos derivados del despliegue de las tecnologías que venden, y si estos ocurren, deben asumir responsabilidad.

En este sentido, y atendiendo el panorama de este informe, las empresas solo deberían desplegar herramientas de tecnología de vigilancia si están en asociación con las autoridades públicas, de conformidad con los principios necesarios y proporcionados, así como con las medidas de transparencia y rendición de cuentas y salvaguardas.

Asimismo, es urgente que tanto Estados como empresas privadas sigan trabajando bajo los Principios Rectores de las Naciones Unidas sobre Empresas y Derechos Humanos y también sobre la labor hecha por el grupo de trabajo intergubernamental de composición abierta del Consejo de Derechos Humanos de las Naciones Unidas sobre las empresas transnacionales y los derechos humanos, especialmente en lo que respecta al desarrollo de un tratado legalmente vinculante sobre empresas y derechos humanos cuyo ámbito de aplicación considera a las empresas transnacionales y nacionales en el mismo nivel. Dicha disposición permitiría que compañías como Hacking Team (Italia) o NSO Group (Israel) sean responsables de proporcionar servicios conocidos por promover abusos contra los derechos humanos a través de la vigilancia estatal.

**::::::**

Este documento fue terminado el 10 de junio del 2019 y es adherido por las siguientes organizaciones de la sociedad civil:

- Hiperderecho (Perú)[37]
- IPANDETEC (Centroamérica)[38]
- Derechos Digitales (América Latina)[39]
- Fundación Karisma (Colombia)[40]
- Coding Rights (Brasil)[41]

[37] https://hiperderecho.org/
[38] https://www.ipandetec.org/
[39] https://www.derechosdigitales.org/
[40] https://karisma.org.co
[41] https://www.codingrights.org/