LOS ARCHIVOS PREDATOR: EMBOSCADA EN LA RED

LA AMENAZA GLOBAL DEL SOFTWARE ESPÍA "REGULADO POR LA UE"

** RESUMEN EJECUTIVO **

AMNISTÍA INTERNACIONAL

Amnistía Internacional es un movimiento integrado por 10 millones de personas que activa el sentido de humanidad dentro de cada una de ellas y que hace campaña en favor de cambios que permitan que todo el mundo disfrute de sus derechos humanos. Nuestra visión es la de un mundo donde quienes están en el poder cumplen sus promesas, respetan el derecho internacional y rinden cuentas. Somos independientes de todo gobierno, ideología política, interés económico y credo religioso, y nuestro trabajo se financia principalmente con las contribuciones de nuestra membresía y con donativos. Creemos que actuar movidos por la solidaridad y la compasión hacia nuestros semejantes en todo el mundo puede hacer mejorar nuestras sociedades.

Publicado por primera vez en 2023
por Amnesty International Ltd
Peter Benenson House, 1 Easton Street
London WC1X 0DW, Reino Unido

Índice: ACT 10/7246/2023
Idioma original: Inglés

amnesty.org

Ilustración de la portada: *© Colin Foo 2023*

AMNISTÍA INTERNACIONAL

RESUMEN EJECUTIVO

Durante la última década, organizaciones de la sociedad civil, personal de investigación y periodistas han expuesto el modo en que gobiernos de todo el mundo vigilaban ilegítimamente a activistas, periodistas y representantes políticos mediante herramientas desarrolladas por empresas privadas de cibervigilancia. Tanto Amnistía Internacional como numerosas organizaciones de la sociedad civil han advertido en repetidas ocasiones de que el comercio y despliegue opacos de tecnologías de vigilancia de fabricación privada —en especial, software espía— por parte de los Estados ha provocado una crisis en materia de vigilancia digital, la cual ha repercutido negativa y gravemente en los derechos humanos, las libertades de los medios de comunicación y los movimientos sociales de todo el mundo. Las revelaciones del Proyecto Pegasus de 2021 —que destaparon la escala y amplitud global de la vigilancia ilegítima facilitada por el software espía Pegasus, de NSO Group— y las posteriores indagaciones de la sociedad civil han obligado a los gobiernos de todo el mundo a tomar nota de la escala y amplitud ingentes del abuso del software espía, lo que ha llevado a adoptar medidas iniciales para frenar a algunos de los distribuidores de software espía más conocidos. Sin embargo, las últimas revelaciones de Amnistía Internacional y las conclusiones de la nueva investigación denominada Archivos Predator, coordinada por la red de medios de comunicación European Investigative Collaborations (EIC), han evidenciado que la acción gubernamental no ha sido ni adecuada ni eficaz para acabar con el abuso del software espía. El presente informe detalla estas conclusiones.

En primer lugar, como parte de la investigación Archivos Predator, el Laboratorio sobre Seguridad de Amnistía Internacional colaboró con EIC —asociación de organizaciones europeas de medios de comunicación— en calidad de socio técnico. Amnistía Internacional analizó documentos a los que había tenido acceso EIC para determinar las especificaciones técnicas de un conjunto de productos de vigilancia desarrollados, operados y comercializados por la alianza Intellexa —formada por empresas de tecnología de vigilancia— entre 2007 y 2022 y descubrió que dicho conjunto incluía infinidad de tecnologías de vigilancia selectiva y masiva.

Las tecnologías de vigilancia selectiva comprenden software espía para móviles altamente invasivo, como Predator, que puede enviarse a los dispositivos mediante ataques de 1 clic o de 0 clics. La alianza Intellexa también ofrece varias técnicas para instalar el software espía mediante “ataques tácticos”, que permiten seleccionar como objetivo dispositivos que se hallan en estrecha proximidad física. Además, Intellexa ha desarrollado, operado y comercializado métodos de infección estratégica, los cuales permiten a un agente estatal dirigir intentos de infección silenciosos a personas usuarias de proveedores de servicios de Internet que cooperen o incluso a todo un país si el operador del software espía tiene acceso directo al tráfico de Internet. Los sistemas de infección estratégica se asemejan a las herramientas de vigilancia masiva, puesto que, para seleccionar como objetivo a una persona e infectarla, precisan tener acceso al tráfico de Internet a gran escala. En los productos de vigilancia masiva ofrecidos por la alianza Intellexa se presupone una evolución de las tecnologías de vigilancia previas, desde sistemas de interceptación legítimos que permitían vigilar el tráfico de forma selectiva e individualizada —lo que en teoría admitía más controles y limitaciones— hasta métodos más amplios e indiscriminados.

Amnistía Internacional cree que ambos tipos de tecnología —software espía altamente invasivo y herramientas de vigilancia masiva indiscriminada— son fundamentalmente incompatibles con los derechos humanos. El software espía Predator y sus variantes bajo denominaciones alternativas son programas espía altamente invasivos que pueden acceder a cantidades ilimitadas de datos de un dispositivo y que, en la actualidad, no pueden auditarse de forma independiente. Por lo tanto, Amnistía Internacional considera que

todo despliegue de Predator y de otras formas de software espía altamente invasivo es incompatible con los derechos humanos y debe prohibirse con carácter permanente.

En segundo lugar, en este informe Amnistía Internacional expone una operación de vigilancia selectiva no revelada hasta la fecha que llevó a cabo un cliente del software espía Predator de Intellexa relacionado con Vietnam. El cliente parece ser afín a los intereses del gobierno de Vietnam y, entre febrero y junio de 2023, seleccionó como objetivo un mínimo de 50 cuentas en redes sociales titularidad de 27 personas y 23 instituciones utilizando para ello herramientas de software espía desarrolladas y comercializadas por la alianza Intellexa. El proceso consistió en enviar ataques de 1 clic a las cuentas de estas personas e instituciones en las redes sociales desde una cuenta en X (antes Twitter) con el nombre @Joseph_Gordon16. Entre los objetivos de esta operación con software espía se cuentan una web de noticias independiente con sede en Berlín, varias personalidades políticas del Parlamento Europeo, la Comisión Europea, personal académico de investigación y grupos consultivos. Además, entre los objetivos fallidos se halla personal de las Naciones Unidas, la presidenta de Taiwán; miembros del Senado y representantes de Estados Unidos, y otras autoridades diplomáticas.

El Grupo de Análisis de Amenazas de Google confirmó a Amnistía Internacional los hallazgos de la propia investigación de Google: los dominios y las URL que Amnistía Internacional había descubierto como parte de la operación de software espía estaban vinculados al sistema de software espía Predator de la alianza Intellexa. Junto con las pruebas aportadas por las entidades asociadas de EIC, en nuestros hallazgos se aprecian indicios de ventas de productos de vigilancia de la alianza Intellexa al Ministerio de Seguridad Pública de Vietnam y se sugiere que detrás de la campaña de software espía podría haber agentes de las autoridades vietnamitas o personas que actúan en su nombre. Además, Google confirmó a entidades asociadas de EIC que "asocian" la campaña de Predator de Intellexa y los indicadores descritos en este informe a "un agente gubernamental de Vietnam".

Estas revelaciones se basan en la investigación técnica que lleva a cabo el Laboratorio sobre Seguridad de Amnistía Internacional para vigilar el desarrollo y despliegue de tecnologías de vigilancia ofrecidas por empresas de software espía mercenario, incluidas aquéllas propuestas por la alianza Intellexa. Como parte de estos esfuerzos, el análisis de Amnistía Internacional sobre la infraestructura técnica reciente ligada al sistema del software espía Predator señala también probables clientes activos o personas objetivo en Sudán, Madagascar, Kazajistán, Mongolia, Egipto, Indonesia, Vietnam y Angola.

Las conclusiones de este informe se basan también en una entrevista con un periodista de Vietnam seleccionado como objetivo, registros de envíos, datos comerciales y otras investigaciones e informes de EIC sobre las ventas de programas de vigilancia e infección de la alianza Intellexa. Amnistía Internacional revisó informes, declaraciones, leyes y estudios de organismos y especialistas de la ONU, autoridades regionales y nacionales a distintos niveles, informes de investigación y sobre políticas de organizaciones de la sociedad civil, así como informes de los medios de comunicación.

En tercer lugar, este informe analiza las implicaciones para los derechos humanos de lo revelado en los Archivos Predator, que muestra cómo se vende y transfiere impunemente en todo el mundo un conjunto de tecnologías de vigilancia altamente invasivas suministradas por la alianza Intellexa. La alianza Intellexa está compuesta por varios proveedores de sistemas de vigilancia que cuentan con presencia empresarial en Estados miembros de la Unión Europea (UE), así como en otros países de todo el mundo. Las revelaciones muestran la escala y amplitud globales de las ventas de tecnologías de vigilancia de una sola alianza de proveedores, que suministró sus productos a Egipto, Libia, Madagascar, Arabia Saudí, Vietnam y Francia —entre muchos otros países— entre 2007 y 2022. Estas transferencias generan una alta probabilidad de violación de los derechos humanos, dados los casos anteriores de vigilancia ilegítima en estos países o la ausencia de salvaguardias nacionales respecto a la vigilancia para impedir que estas tecnologías se usen ilegítimamente contra la sociedad civil, periodistas o figuras de la oposición política.

En cuarto lugar, este informe detalla un historial de abusos contra los derechos humanos que se han vinculado con la alianza Intellexa en Grecia, Libia y Egipto. Intellexa se publicita como una "empresa regulada y radicada en la UE". Según informes, la alianza Intellexa se compone de Nexa Technologies y Advanced Middle East Systems (que integran el grupo Nexa), así como de WiSpear, Cytrox y Senpai Technologies (que conforman el grupo Intellexa). Los grupos de empresas Nexa e Intellexa controlan múltiples entidades corporativas, algunas de las cuales han cambiado de denominación. Las entidades operan en varias jurisdicciones, tanto dentro como fuera de la UE. La naturaleza exacta de los vínculos entre estas empresas está inmersa en el secretismo, ya que las entidades corporativas y las estructuras entre ellas se transforman, se rebautizan, cambian de marca y evolucionan constantemente. Estas estructuras corporativas opacas y complejas parecen facilitar que las empresas eludan la rendición de cuentas, la transparencia y la normativa gubernamental, incluidos los controles de exportación regionales y nacionales,

así como los mecanismos de diligencia debida corporativa. En el caso de la alianza Intellexa, el panorama es aún más complejo, debido a las estructuras corporativas no sólo de una empresa principal, sino de los distribuidores de productos de vigilancia aliados, sus empresas matrices y sus inversores. La naturaleza enrevesada de esta entidad corporativa podría dificultar aún más la rendición de cuentas y la transparencia en lo que respecta a la vigilancia selectiva ilegítima que se practica con herramientas de esta alianza.

Tal como se establece en los Principios Rectores de la ONU sobre las Empresas y los Derechos Humanos (Principios Rectores de la ONU), las empresas tienen también la responsabilidad de respetar los derechos humanos con independencia del lugar del mundo en el que operen. Para hacer frente a esa responsabilidad, las empresas deben ejercer la diligencia debida en materia de derechos humanos. Las propias empresas de la alianza Intellexa no han revelado con carácter proactivo ninguna información sobre sus prácticas de diligencia debida en materia de derechos humanos. Cualquier evaluación —si es que existe— sobre el impacto de sus tecnologías de vigilancia en los derechos humanos es un misterio. En virtud del derecho internacional de los derechos humanos, los Estados están también obligados a proteger los derechos humanos de abusos perpetrados por terceros. Esto incluye la obligación de regular la conducta de las empresas que están domiciliadas en su territorio o bajo su control efectivo para impedir que cometan o contribuyan a cometer abusos contra los derechos humanos, incluso en el caso de que éstos se produzcan en otros países. La incapacidad de los Estados para ejercer un control significativo sobre la alianza Intellexa —por ejemplo, los Estados donde tienen su sede las entidades corporativas de la alianza, entre ellos Grecia, Irlanda, Francia, Alemania, República Checa, Chipre, Hungría, Suiza, Israel, Macedonia del Norte y Emiratos Árabes Unidos— ha dado paso a violaciones de los derechos humanos. En conjunto, las conclusiones ya mencionadas muestran que sociedad civil y periodistas siguen afrontando las devastadoras consecuencias del uso ilegítimo e incontrolado de tecnologías de vigilancia, que continúan amenazando los derechos a la privacidad y a la libertad de expresión, de asociación y de reunión pacífica de las personas afectadas. Además, como se detalla en este informe, la selección de autoridades oficiales regionales, nacionales e internacionales como objetivo demuestra una vez más que el software espía comercial tiene graves consecuencias tanto para los derechos humanos como para la seguridad del ecosistema digital. En ausencia de normativa, estas tecnologías de vigilancia pueden volverse contra terceros gobiernos y autoridades, como ya ha sucedido.

Estos hallazgos son sólo la punta del iceberg. Dado que las empresas de vigilancia y sus clientes estatales siguen ocultándose tras la retórica de la seguridad nacional y la confidencialidad para eludir la transparencia y la rendición de cuentas, es probable que la escala y el alcance reales de la vigilancia ilegítima mediante herramientas suministradas por la alianza Intellexa sean mucho mayores. Las advertencias de la sociedad civil y las lecciones aprendidas del Proyecto Pegasus significan que, en cada uno de los países en los que las revelaciones muestran que la alianza Intellexa ha vendido sus tecnologías, la sociedad civil podría estar sometida a una vigilancia clandestina generalizada. Estas nuevas revelaciones dejan patente, una vez más, que la venta y transferencia descontrolada de tecnologías de vigilancia podría seguir facilitando abusos contra los derechos humanos a escala global y masiva, puesto que se sigue permitiendo a las empresas vender y transferir libremente sus productos en el más absoluto secreto. Nuestros hallazgos demuestran una vez más que cualquier afirmación por parte de las empresas de que la vigilancia ilegítima es esporádica es rotundamente falsa. Los abusos contra los derechos humanos son la norma del sector, no una excepción.

Tras las revelaciones del Proyecto Pegasus, los Estados han dado algunos pasos con vistas a regular el sector y el uso estatal de estas tecnologías. Algunos avances son significativos y van en la dirección correcta. Sin embargo, las declaraciones públicas, las recomendaciones y los compromisos voluntarios no siempre se han convertido en acciones, y aún no se han rendido cuentas ni se ha ofrecido resarcimiento a las personas que, en todo el mundo, han sido seleccionadas ilegítimamente como objetivo de software espía. Si bien algunos Estados han emprendido iniciativas voluntarias, otros han obstruido las investigaciones y no han proporcionado una transparencia significativa. Es necesario que los Estados lleven a cabo más esfuerzos concertados para establecer salvaguardias de derechos humanos que sean vinculantes y aplicables a nivel nacional, regional e internacional. En 2019, el anterior relator especial de las Naciones Unidas sobre la libertad de opinión y de expresión indicó: “Decir que todo un sistema completo de control y utilización de tecnologías de vigilancia selectiva ha dejado de funcionar ni siquiera se acerca a la realidad. La realidad es que apenas existe”. Amnistía Internacional cree que, a pesar de los progresos iniciales, la situación no ha variado.

En particular, las últimas revelaciones plasman un panorama desolador en lo que respecta a la inacción de la UE y sus Estados miembros a la hora de frenar a las empresas que no rinden cuentas y a los Estados miembros díscolos, que siguen aprovechándose de las grietas, visiblemente grandes, de los sistemas normativos a nivel regional y nacional. La descarada campaña de vigilancia que se detalla en este informe, efectuada con las herramientas de la alianza Intellexa, muestra los riesgos muy directos de la proliferación y

transferencia sin control de herramientas de cibervigilancia desde países de la UE. No sólo conducen a abusos contra los derechos humanos fuera de la Unión, sino que también suponen una amenaza para la seguridad y los derechos humanos dentro de ella.

Las exportaciones de software espía desde la UE están sujetas a la concesión de licencias en virtud del Reglamento relativo a las exportaciones de productos de doble uso, para la cual, en teoría, deberían tenerse en cuenta los riesgos para los derechos humanos que plantean dichas exportaciones. Sin embargo, las revelaciones de los Archivos Predator demuestran que los Estados miembros concedieron licencias de exportación para tecnologías de vigilancia cuando existía un riesgo sustancial de que los usuarios finales cometieran violaciones de derechos humanos. Las revelaciones muestran también que la normativa europea de control de las exportaciones se eludió a través de estructuras corporativas opacas y entidades en terceros países. Queda claro que el Reglamento europeo relativo a las exportaciones de productos de doble uso presenta carencias importantes. Dos años después de publicarse el Reglamento refundido relativo a las exportaciones de productos de doble uso, éste no se ha aplicado de forma sólida y transparente. La Comisión de Investigación Encargada de Examinar el Uso del Programa Espía de Vigilancia Pegasus y Otros Programas Equivalentes (Comisión PEGA) del Parlamento Europeo ha señalado también la falta de voluntad política de la UE y los Estados miembros. Aunque los esfuerzos legislativos en curso, como la Propuesta de directiva sobre la diligencia debida de las empresas en materia de sostenibilidad, ofrecen una acertada oportunidad para empezar a abordar los daños del sector de la vigilancia selectiva, las lagunas de las propuestas presentadas por las entidades colegisladoras de la UE podrían significar que dicha directiva no se aplique correctamente a las empresas que comercializan tecnología de vigilancia.

RECOMENDACIONES CLAVE A LOS ESTADOS

Vista la ineficacia de la normativa actual, así como la naturaleza intrínsecamente abusiva de Predator, todos los Estados deberían:

- (especialmente los Estados que han concedido licencias de exportación) revocar inmediatamente todas las licencias de comercialización y exportación concedidas a la alianza Intellexa y llevar a cabo una investigación independiente, imparcial y transparente para determinar el alcance de la selección ilegítima de objetivos, que culmine con una declaración pública sobre los resultados de los esfuerzos realizados y las medidas tomadas para prevenir futuros daños.
- Hacer cumplir la prohibición del uso de software espía altamente invasivo. En la actualidad, dicho software espía no puede ser auditado de forma independiente y su funcionamiento no puede limitarse sólo a las funciones necesarias y proporcionadas a un uso y un objetivo específicos.
- Implantar un marco normativo de derechos humanos que regule la vigilancia y que sea conforme a las normas internacionales de derechos humanos. Hasta que exista un marco de este tipo, debería dictarse una moratoria sobre la compra, venta, transferencia y uso de todos los programas espía.
- Aplicar una legislación nacional que imponga salvaguardias contra las violaciones de derechos humanos y los abusos cometidos a través de la vigilancia digital y establecer mecanismos de rendición de cuentas que proporcionen a las víctimas de abusos de vigilancia una vía de recurso.
- Exigir legalmente a las empresas de vigilancia que ejerzan la diligencia debida en materia de derechos humanos en relación con sus operaciones globales, incluido el uso de sus productos y servicios.

RECOMENDACIONES CLAVE A LA UNIÓN EUROPEA Y SUS ESTADOS MIEMBROS

- Los Estados miembros de la UE y a la Comisión Europea deberían garantizar una aplicación firme del Reglamento de la UE de control de las exportaciones de 2021. Esto incluye tomar medidas inmediatas para subrayar la obligación de ejercer la diligencia debida en materia de derechos humanos derivada del Reglamento sobre exportaciones de doble uso y crear un mercado transparente de tecnologías de cibervigilancia sujeto a salvaguardias efectivas de derechos humanos.
- Los Estados miembros de la UE deben adoptar y hacer cumplir una legislación que exija a todos los actores empresariales el respeto de los derechos humanos y la aplicación de medidas de diligencia debida en materia de derechos humanos acordes con los Principios Rectores de la ONU. Como parte de las deliberaciones en curso en torno a la Propuesta de directiva sobre la diligencia debida de las empresas en materia de sostenibilidad, la UE debe exigir a las empresas que ejerzan la diligencia debida en materia de derechos humanos con respecto a toda la cadena de valor, incluidos la compra, la venta, la transferencia, la exportación y el uso de los productos. Las empresas que operan en cualquier sector —incluidas las que producen software espía, así como las instituciones financieras— deberían aplicar los requisitos de la citada propuesta de directiva.

RECOMENDACIONES CLAVE AL GOBIERNO DE VIETNAM

El gobierno de Vietnam debe llevar a cabo una investigación independiente, imparcial y transparente sobre la vigilancia selectiva ilegítima mencionada en este informe, incluidas averiguaciones para determinar si existen vínculos entre esta campaña de software espía y alguna agencia gubernamental específica.

RECOMENDACIONES CLAVE A LA ALIANZA INTELLEXA

La alianza Intellexa debe poner fin a la producción y venta de Predator y de cualquier otro software espía altamente invasivo similar que no incluya salvaguardias técnicas que permitan su uso legítimo en virtud de un marco normativo que respete los derechos humanos. También debería proporcionar una indemnización adecuada u otras formas de resarcimiento efectivo a las víctimas de vigilancia ilegítima.

AMNISTÍA INTERNACIONAL ES UN MOVIMIENTO GLOBAL DE DERECHOS HUMANOS. LAS INJUSTICIAS QUE AFECTAN A UNA SOLA PERSONA NOS AFECTAN A TODAS LAS DEMÁS.

CONTÁCTANOS


info@amnesty.org


+44 (0)20 7413 5500

ÚNETE A LA CONVERSACIÓN


www.facebook.com/AmnistiaAmericas


@Amnistía