



“EMPEZAMOS POR LA SENTENCIA”

DENTRO DE LA MAQUINARIA DE VIGILANCIA DE MARRUECOS
RESUMEN EJECUTIVO

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.

© Amnesty International 2026

Salvo cuando se indique lo contrario, el contenido de este documento está protegido por una licencia 4.0 de Creative Commons (atribución, no comercial, sin obra derivada, internacional).

<https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.es>

Para más información, visiten la página *Permisos* de nuestro sitio web:

<https://www.amnesty.org/es/permissions/>.

El material atribuido a titulares de derechos de autor distintos de Amnistía Internacional no está protegido por la licencia Creative Commons.

Publicado por primera vez en 2020

por Amnesty International Ltd.

Peter Benenson House, 1 Easton Street

London WC1X 0DW, Reino Unido

Índice: MDE 29/1481/2026 Spanish

Idioma original: inglés

amnesty.org



Imagen de portada: © Rectangle / Evan Grothjan

**AMNISTÍA
INTERNACIONAL**



RESUMEN EJECUTIVO

“Hay leyes escritas, pero no se aplican. Hay leyes que nadie respeta. No les importan las autorizaciones ni las órdenes judiciales. A veces incluso se pueden redactar los documentos *a posteriori*, hacer las cosas al revés. Hay impunidad total. Empezamos por la sentencia.”

Safir, exmiembro de la Dirección General de Vigilancia del Territorio (DGST).

“Una prueba”, “un conejillo de indias”, así describieron los agentes de los servicios de inteligencia nacional de Marruecos, la Dirección General de Vigilancia del Territorio (*Direction Générale de la Surveillance du Territoire*, DGST), al defensor de los derechos humanos y profesor Maâti Monjib cuando lo eligieron como una de las primeras personas a las que atacar con el programa espía Pegasus de NSO Group en 2017. Pero para Maâti Monjib, el resultado fue cualquier cosa menos teórico. El hecho de que la DGST lo eligiera como objetivo confirmó lo que él llevaba mucho tiempo sospechando: las autoridades marroquíes lo vigilaban por su labor de derechos humanos y sus escritos académicos. También dejó al descubierto ante las autoridades toda su vida digital: sus mensajes, llamadas, cámara, ubicación y contactos, entre otras cosas. Al mismo tiempo, Maâti Monjib se enfrentaba a enjuiciamiento por la vía penal y a represión por su trabajo. En 2015, fue sometido a un juicio penal por cargos de recibir fondos extranjeros para impartir formación a periodistas y se le prohibió salir de Marruecos. Años más tarde, fue condenado a un año de prisión. En 2020 volvió a ser objeto de cargos falsos relacionados con blanqueo de dinero y malversación, y Amnistía Internacional pidió su puesta en libertad inmediata e incondicional. Durante ese período, fue sometido a implacables campañas de desprestigio promovidas por medios de comunicación y comentaristas de Internet afines al Estado. Aunque finalmente fue indultado en 2024, el acoso no cesó. Todavía en 2025, circularon en Internet vídeos suyos en los que se afirmaba que bebía alcohol, fumaba *shisha* y “se solazaba con sus amantes”. Maâti Monjib cree que la estrategia consistía no sólo en silenciarlo a él, sino también en atemorizar a otras personas para que guardaran silencio. Como él mismo dijo, parafraseando un proverbio marroquí: “Golpea a los grandes y los pequeños tendrán miedo”.

La experiencia de Maâti Monjib no es ni mucho menos excepcional. Sólo por ejercer sus derechos, los defensores y defensoras de los derechos humanos marroquíes suelen ser víctimas de una combinación de vigilancia ilícita, campañas de desprestigio y acoso judicial o enjuiciamiento penal. Los agentes de la DGST actúan sin supervisión judicial ni rendición de cuentas y se centran, en secreto y con impunidad, en quienes discrepan. La variedad de instrumentos que utilizan es amplia, pero el objetivo es claro: chantajear, desacreditar, avergonzar y, si es necesario, encarcelar a quienes alzan la voz en defensa de los derechos humanos en Marruecos.

Este informe ofrece la imagen más detallada y completa realizada hasta la fecha del ecosistema de vigilancia que permite a las autoridades marroquíes utilizar tácticas represivas para acosar, desacreditar y, a la larga, silenciar a los defensores y defensoras de los derechos humanos. Se basa en nuevos testimonios de fuentes

que han trabajado en los servicios de inteligencia marroquíes y que participaron en la vigilancia ilícita de defensores y defensoras de los derechos humanos, en datos de vigilancia filtrados y registros de selección de objetivos internos del gobierno, en material filtrado de proveedores de servicios de vigilancia y en investigaciones periodísticas originales llevadas a cabo por socios de investigación de Amnistía Internacional.

Con la revelación de pruebas de ataques con el programa espía de Hacking Team en 2012, Marruecos fue uno de los primeros países en los que se descubrió que activistas y periodistas eran objeto de ataques con herramientas avanzadas de software espía. La sociedad civil marroquí volvió a figurar entre el conjunto mundial de objetivos del programa espía Pegasus en 2019, y el amplio alcance de la vigilancia ejercida por Marruecos contra defensores y defensoras de los derechos humanos salió a la luz durante el Proyecto Pegasus de 2021. Este historial documentado de uso indebido de software espía y de la vigilancia convierte a Marruecos en un caso excepcional para analizar cómo los Estados se sirven de diversas tecnologías de vigilancia para atacar a personas críticas y limitar el trabajo de la sociedad civil.

El ecosistema de vigilancia de Marruecos se basa en herramientas de alta tecnología, incluidos programas espía altamente invasivos como Pegasus, así como en técnicas más tradicionales, como seguir al objetivo en persona, grabar conversaciones y otros métodos similares. Los dispositivos personales no son seguros. Se graba en secreto a las personas en vídeo y audio cuando están detenidas, en sus oficinas y automóviles, e incluso en su dormitorio. Las llamadas telefónicas se graban y se espían sistemáticamente. Se rastrean los datos de ubicación, que revelan los desplazamientos diarios, los contactos y otro tipo de información. Las tiendas de telefonía venden teléfonos móviles previamente infectados con programas maliciosos (*malware*) por agentes de la DGST. Se recluta a vecinos como informantes para que comuniquen los desplazamientos y actividades cotidianos de los defensores y defensoras de los derechos humanos. Todas estas tácticas se aplican no sólo a los defensores y defensoras de los derechos humanos que son objeto de vigilancia, sino también a sus familiares, amistades y redes profesionales, tanto dentro de Marruecos como en el extranjero. En resumen, para quienes defienden los derechos humanos en Marruecos, no hay dónde esconderse ni forma de escapar de la omnipresente red de vigilancia del Estado.

Como resultado, los detalles más íntimos de la vida de los defensores y defensoras de los derechos humanos son un libro abierto para las autoridades, que pueden servirse de ellos para silenciarlos. Pueden capturar datos, incluidas grabaciones de vídeo y audio de carácter personal, íntimo o sexual, y en ocasiones los comparten con medios de comunicación afines al Estado, que llevan a cabo campañas públicas de desprestigio con el objetivo de mancillar la reputación de los y las activistas y desacreditarlos ante la opinión pública marroquí. Las defensoras de los derechos humanos en particular, o las mujeres relacionadas con hombres que son objetivos destacados de ataques, son sometidas a campañas con las que se intenta humillarlas públicamente por infracciones reales o supuestas de normas sociales conservadoras. Estas operaciones pueden prolongarse durante años y son promovidas en Internet por un ejército de comentaristas afines al Estado para aumentar el alcance y la visibilidad de los contenidos. Son tan comunes que los medios a través de los cuales se llevan a cabo con mayor frecuencia reciben localmente el nombre de “medios de difamación”.

Además de la vigilancia ilícita y las campañas de desprestigio, los defensores y defensoras de los derechos humanos han sido objeto de forma reiterada de acoso judicial y de acusaciones de motivación política o falsas, detención y encarcelamiento tras juicios sin garantías y sobre la base de un marco jurídico que infringe las normas internacionales. Algunas de estas personas han sido enjuiciadas por actos protegidos por su derecho a la libertad de expresión o de asociación, por cargos que no constituyen delitos reconocibles en virtud del derecho internacional, como los delitos relacionados con la expresión que, definidos en términos amplios, se utilizan para enjuiciar a personas por expresar su disidencia o por otras formas de expresión legítimas. En algunos casos, se presiona a los defensores y defensoras de los derechos humanos para que presten falso testimonio contra otras personas.

La persecución de los defensores y defensoras no se circunscribe a las fronteras de Marruecos. Las personas que están en el exilio, o que informan desde otros países, siguen siendo objeto de vigilancia y de campañas de desprestigio. Incluso se ha captado a funcionarios y diplomáticos extranjeros.

El resultado más general de estas tácticas combinadas es la creación de un profundo efecto intimidatorio en otros defensores y defensoras de los derechos humanos, así como en cualquier otra posible disidencia en el seno de la sociedad en general. Al no haber medio de saber cuándo están siendo observados y grabados, enfrentándose a riesgos desconocidos para sus familiares y amistades, temiendo el escarnio público o incluso el encarcelamiento si alzan la voz, el costo de la disidencia en Marruecos es cada vez mayor.

Sin embargo, muchas personas siguen alzando la voz e intentando que quienes ejercen el poder rindan cuentas. Sus casos se destacan en este informe. Sus historias subrayan la necesidad urgente de que

Marruecos ponga fin a la impunidad de que goza la DGST, reforme sus leyes y prácticas y respete, proteja y haga efectivos los derechos humanos de los y las periodistas y de quienes defienden estos derechos.

EL USO DE LA VIGILANCIA ILÍCITA EN MARRUECOS

La vigilancia encubierta no constituye en sí misma una violación de derechos humanos. Puede llevarse a cabo de forma lícita siempre que se cumplan una serie de garantías, establecidas en el Pacto Internacional de Derechos Civiles y Políticos, en el que Marruecos es parte, y relacionadas con la protección del derecho a la privacidad y a la libertad de opinión y de expresión. El Comité de Derechos Humanos determinó que el derecho a la privacidad exigía la existencia de sistemas de supervisión sólidos e independientes en relación con la vigilancia, la interceptación y el hackeo. La Asamblea General de la ONU, en su resolución 73/179, señaló que la vigilancia de las comunicaciones digitales debe ser compatible con las obligaciones internacionales en materia de derechos humanos y debe llevarse a cabo sobre la base de un marco jurídico que sea de acceso público, claro, preciso, amplio y no discriminatorio.

La vigilancia es ilícita incluso cuando se lleva a cabo de acuerdo con los procedimientos jurídicos nacionales si estos procedimientos vulneran o contravienen las normas internacionales de derechos humanos. La vigilancia es ilícita, por ejemplo, cuando se lleva a cabo sin la autorización y la supervisión judiciales que exigen los procedimientos que regulan su uso.

Con arreglo al derecho internacional de los derechos humanos, Marruecos no sólo debe abstenerse de cometer violaciones de derechos humanos, sino que también debe proteger a las personas frente a los abusos cometidos por actores privados. Además, Marruecos no sólo debe garantizar la legalidad de la vigilancia realizada dentro de sus fronteras, sino también fuera del país. El uso de software espía y otras herramientas de vigilancia como mecanismos de represión transnacional ha sido señalado cada vez más como motivo de preocupación por una lista en aumento de autoridades y personas expertas de la ONU.

En Marruecos, la vigilancia corre a cargo de la DGST, a menudo sin autorización judicial y con el propósito ilícito de atacar a los defensores y defensoras de los derechos humanos por su labor. Esta vigilancia se extiende no sólo a los propios defensores y defensoras, sino también a sus familiares, representantes legales y redes sociales y profesionales. Se lleva a cabo sin supervisión independiente y, por lo general, sin tener en cuenta los procedimientos jurídicos nacionales.

En virtud del derecho y las normas internacionales, las injerencias en el derecho a la privacidad sólo están permitidas cuando cumplen los requisitos de legalidad, necesidad y proporcionalidad y se llevan a cabo con un fin legítimo. Por tanto, la vigilancia que se lleva a cabo para atacar a defensores y defensoras de los derechos humanos por su labor de defensa de estos derechos es ilícita en virtud del derecho y las normas internacionales de derechos humanos, independientemente de si cumple o no los requisitos que establezcan los procedimientos jurídicos nacionales.

Para cumplir con su obligación de respetar el derecho a la privacidad, es fundamental que las autoridades cuenten con salvaguardias jurídicas y de otro tipo que permitan evitar el uso indebido de tecnologías de vigilancia en la práctica. La falta de una supervisión judicial adecuada, de medidas de rendición de cuentas o de acceso a un recurso efectivo no sólo da lugar a violaciones del derecho a la privacidad de las personas que son objeto de vigilancia, sino que también crea un efecto intimidatorio que impulsa a periodistas, activistas, defensores y defensoras de los derechos humanos y muchos otros miembros de la comunidad a limitar su libertad de expresión, sus informaciones o su activismo, reduciendo de ese modo el espacio cívico para todas las personas.

Aunque la responsabilidad principal de hacer respetar el derecho de los derechos humanos recae sobre Marruecos, las empresas privadas, tanto nacionales como internacionales, también tienen responsabilidades en materia de derechos humanos para evitar causar abusos contra estos derechos o contribuir a ellos. Estas obligaciones están por encima de la legislación nacional.

La compatibilidad de las medidas de vigilancia con el derecho de los derechos humanos no depende únicamente de las leyes y de las prácticas de los organismos estatales, sino también de las herramientas concretas que se utilicen. La vigilancia masiva, tal como se lleva a cabo utilizando herramientas como las adquiridas a Amesys o Verint, o mediante la cooperación extralegal de proveedores de telecomunicaciones, es contraria al derecho y las normas de derechos humanos. Muchos tipos de software espía moderno altamente invasivo utilizados por las autoridades marroquíes, como Pegasus de NSO Group y Remote Control System (RCS) de Hacking Team, son radicalmente incompatibles con los derechos humanos debido a su diseño. Amnistía Internacional ha pedido la prohibición en todo el mundo de estos tipos de software espía altamente invasivo, porque permiten el acceso ilimitado a los dispositivos y su uso no puede auditarse de forma independiente.

Además, el derecho a la privacidad y otros derechos humanos pueden violarse mediante el uso de diversas herramientas, aunque sus proveedores o usuarios no las consideren herramientas de “vigilancia” en sentido estricto. Esto incluye herramientas de análisis forense digital, captadores IMSI, etc. La legalidad de la vigilancia tampoco depende de la sofisticación técnica de los dispositivos utilizados. Incluso el simple acto de grabar o escuchar a una persona elegida como objetivo debe ajustarse al derecho y las normas internacionales de derechos humanos.

DENTRO DE PEGASUS: CÓMO HA EVOLUCIONADO EL PROGRAMA ESPÍA MÁS CONOCIDO DEL MUNDO Y CÓMO LO HA UTILIZADO MARRUECOS PARA ATACAR A DEFENSORES Y DEFENSORAS DE LOS DERECHOS HUMANOS Y PERIODISTAS

Durante años, el programa espía Pegasus de NSO Group se ha utilizado para facilitar la comisión de violaciones de derechos humanos en gran escala en todo el mundo. Como parte de este informe, Amnistía Internacional hizo uso de material de marketing interno y material técnico de NSO Group no publicados anteriormente, que se revelaron en el marco de un prolongado procedimiento judicial entablado por la vía civil en Estados Unidos por WhatsApp y Meta y que ofrecen la imagen más completa hasta la fecha de cómo se diseña, utiliza y mantiene el sistema de Pegasus.

Este nuevo análisis ofrece conclusiones valiosas sobre la rendición de cuentas en relación con los programas espía, entre ellas una descripción de hasta qué punto el sistema utilizado por los clientes gubernamentales requiere un mantenimiento y una asistencia continuos por parte de NSO Group para que puedan seguir funcionando. Los documentos recién revelados también corroboran de forma independiente la autenticidad y exactitud del conjunto de datos filtrado que sirvió de base para la investigación original del Proyecto Pegasus.

Este mejor conocimiento de Pegasus ha permitido a Amnistía Internacional ampliar sus informes anteriores sobre el uso del programa espía de NSO Group en Marruecos. El presente informe documenta que, a pesar de los desmentidos oficiales, las autoridades marroquíes utilizaron el programa espía Pegasus entre 2017 y 2021, y posiblemente más tarde. Amnistía Internacional documenta cómo el uso de Pegasus en Marruecos evolucionó paralelamente a los avances de la propia tecnología. Las pruebas periciales acreditan cómo se utilizaron diversos “vectores”, como explotación de vulnerabilidades (*exploits*) y técnicas de infección, para atacar los dispositivos de defensores y defensoras de los derechos humanos, entre ellos: “Ataques de 1 clic”, que normalmente se basan en que la víctima haga clic en un enlace malicioso; “ataques de 0 clics”, que pueden infectar subrepticiamente a un objetivo sin que éste tenga que hacer clic en un enlace ni, de hecho, realizar ninguna acción, y ataques de inyección de red, que dependían del uso de la red de Maroc Telecom.

Sobre la base de la documentación interna de NSO Group mencionada anteriormente, en el presente informe se acreditan los pasos que sigue la empresa para registrar una infraestructura de ataque específica para cada cliente. Este hallazgo valida la metodología de la comunidad de rendición de cuentas sobre el software espía a la hora de vincular grupos de ataques con programas espía con el mismo operador, lo cual reviste especial importancia en el caso del uso de la herramienta por las autoridades marroquíes, ya que permitiría establecer que el mismo cliente es responsable no sólo de los ataques contra defensores y defensoras de los derechos humanos en Marruecos, sino también de los ataques de vigilancia ilícita con el programa espía Pegasus contra activistas y periodistas marroquíes que viven en el extranjero, así como contra determinados activistas, periodistas, diplomáticos y otros funcionarios que son ciudadanos de otros países.

CÓMO UNA OSCURA RED DE EMPRESAS DE VIGILANCIA FACILITA DIVERSAS TÉCNICAS DE VIGILANCIA EN MARRUECOS

Aunque el uso del programa espía Pegasus por las autoridades marroquíes es de gran importancia, habida cuenta de las capacidades y los efectos de los programas espía altamente invasivos, se trata sólo de una de las muchas herramientas digitales del ecosistema de vigilancia represiva de Marruecos. El gobierno marroquí recurre a una diversidad de técnicas, así como a herramientas adquiridas, sin escrutinio público, a diversos actores empresariales con sede en Israel, la Unión Europea y Estados Unidos. También cuenta con la cooperación extrajudicial de al menos un proveedor nacional de telecomunicaciones.

Este informe documenta que, además de los contratos con NSO Group, dos organismos de seguridad marroquíes, la DGST y el Consejo Superior de la Defensa Nacional (*Conseil Supérieur de la Défense Nationale*, CSDN), habían suscrito contratos con la ya desaparecida empresa italiana de software espía Hacking Team (posteriormente rebautizada como Memento Labs) desde al menos 2009. Marruecos fue uno de los principales clientes del programa espía Remote Control System (RCS) de esa empresa.

Investigaciones de otras organizaciones de la sociedad civil también han identificado casos de uso en Marruecos del programa espía FinSpy, producido por la red británico-alemana de empresas Gamma Group y FinFisher.

Además de las tecnologías de vigilancia selectiva, Marruecos ha utilizado varias tecnologías de vigilancia masiva que permiten el seguimiento, la interceptación, el almacenamiento o el análisis generalizados y masivos de los materiales de las personas usuarias. Por ejemplo, desde diciembre de 2009, Marruecos ha utilizado el sistema Eagle (después rebautizado como Cerebro) de la empresa francesa de telecomunicaciones y defensa Amesys (posteriormente rebautizada como Nexa Technologies y, más tarde, como Trovicor Intelligence, para volver a cambiar su nombre por el de Datafusion en 2024). Esta tecnología permite hacer el seguimiento del tráfico de Internet (IP) a escala nacional. El proyecto, denominado “Popcorn” por Amesys, implicó la introducción de la tecnología Cerebro de interceptación masiva de Internet en Marruecos.

El informe documenta también la compra por Marruecos en 2014 del sistema Reliant 12 de la empresa estadounidense Verint, que permite la recopilación y el análisis unificados de las comunicaciones telefónicas, los datos de los proveedores de servicios de Internet móvil y los datos del tráfico de Internet.

La DGST ha utilizado captadores IMSI, unos dispositivos diseñados para reproducir antenas de telefonía móvil y que pueden captar los datos de dispositivos cercanos, incluso de aplicaciones de mensajería cifrada antes de su transmisión, lo que permite a los agentes espiar los teléfonos de activistas y vigilar a defensores y defensoras de los derechos humanos.

La DGST también ha recurrido al dispositivo universal de extracción forense UFED, de la empresa israelí Cellebrite. Esta herramienta de vigilancia permite el acceso total a los datos de un dispositivo mientras está bajo la custodia física de un operador. Las autoridades han aprovechado situaciones como la detención o el tránsito en aeropuertos para acceder ilícitamente a dispositivos de defensores y defensoras de los derechos humanos sin su conocimiento.

Marruecos también es cliente de la empresa de ciberinteligencia Cognyte, que se escindió en 2021 de la empresa estadounidense Verint Systems y cuyas herramientas permiten a los clientes controlar cuentas falsas de redes sociales (“avatares”) para reunir información sobre los usuarios de las redes sociales o para lanzar ataques de ingeniería social.

Según el exagente de la DGST *Safir*, un elemento esencial de las capacidades de vigilancia de este organismo es la cooperación de un proveedor de telecomunicaciones nacional. *Safir* explicó que los agentes de la DGST tienen acceso directo a los datos y las comunicaciones a través de la red, incluido el acceso a las llamadas, que los agentes pueden escuchar o transcribir a su voluntad. Las capacidades de vigilancia descritas son compatibles con las funcionalidades que ofrece el producto RELIANT de Verint, un sistema de vigilancia masiva que se vendió a las autoridades marroquíes a mediados de la década de 2010, según los registros de ventas internos de Verint. Los registros de ventas también mencionan a Maroc Telecom como posible comprador de productos de interceptación de redes de Verint en tanto que parte del sistema en general. Investigaciones periciales han confirmado que la red de Maroc Telecom se ha utilizado para facilitar ataques de software espía mediante una técnica conocida como “inyección de red”.

El acceso no regulado a infraestructuras y datos de telecomunicaciones privados también ha permitido a la DGST llevar a cabo ataques de inyección de red para instalar software espía y rastrear libremente los datos de ubicación. Al proporcionar información técnica de identificación a la DGST al margen de los procesos legales, este proveedor también facilita la vigilancia ilícita por parte de la DGST.

La DGST y otros organismos también recurren a herramientas menos sofisticadas tecnológicamente, como dispositivos ocultos de grabación de audio y vídeo colocados en viviendas, automóviles, oficinas, espacios públicos y lugares de detención. Los localizadores GPS pueden seguir la ubicación de un objetivo a lo largo del tiempo, y los agentes de la DGST pueden verla a través de su propia interfaz personalizada. Estas técnicas se utilizan en combinación con el reclutamiento de personas del entorno de defensores y defensoras de los derechos humanos que son objeto de vigilancia ilícita o con acceso a ellos, por ejemplo, personal de cafeterías, comerciantes locales o vecinos, para que informen sobre sus actividades.

Los agentes de la DGST también llevan a cabo videovigilancia a través de redes de cámaras de vídeo públicas, y pueden acceder a cámaras privadas mediante una herramienta llamada NightHawk, un

dispositivo del tamaño de una maleta pequeña fabricado por la empresa israelí de ciberinteligencia Interionet.

Para desplegar este conjunto de herramientas, la DGST se apoya en organismos asociados y en multitud de técnicas. Por ejemplo, el software espía RCS se instaló mediante la infección física de dispositivos, a menudo a través de memorias USB, durante, por ejemplo, traslados al aeropuerto o en cibercafés.

El software espía también se ha utilizado preinstalándolo en dispositivos móviles que luego se colocan en tiendas y se venden a los objetivos.

Aunque es indudable que la aplicación de prácticas sólidas de seguridad digital puede dificultar la vigilancia de quienes defienden los derechos humanos por parte de la DGST, dado el uso de tantas técnicas, puede resultar casi imposible escapar de este ecosistema de vigilancia más amplio.

EL USO DE CAMPAÑAS DE DESPRESTIGIO PARA DESACREDITAR A LOS DEFENSORES Y DEFENSORAS DE LOS DERECHOS HUMANOS

Este informe documenta que uno de los objetivos principales de la vigilancia ilícita de defensores y defensoras de los derechos humanos es desacreditarlos públicamente.

En varios casos documentados en el informe, la información privada recopilada a través de las operaciones de vigilancia de la DGST contra defensores y defensoras de los derechos humanos apareció posteriormente en informaciones de medios de comunicación y se utilizó en campañas coordinadas de desprestigio contra estas personas. En muchos casos, estas campañas corrían a cargo de medios de comunicación políticamente afines a las autoridades, como Chouf TV, Barlamane y Le360, y a menudo incluían imágenes y vídeos privados de los objetivos. Se recurrió a campañas de desprestigio de carácter sexual para intentar desacreditar a defensoras de los derechos humanos o, en particular, a mujeres vinculadas con destacados periodistas y defensores de los derechos humanos. Aunque Amnistía Internacional no ha podido verificar de forma independiente la fuente de la información revelada por estos medios de comunicación, la naturaleza del material, que incluye imágenes íntimas y comunicaciones privadas, y la aparente ausencia de cualquier otra vía plausible de acceso de estos medios de comunicación a él plantean graves motivos de preocupación, en el sentido de que las autoridades marroquíes puedan haber revelado, compartido o puesto a disposición de los medios de comunicación la información obtenida mediante vigilancia.

Estas campañas se amplifican en Internet. Meta, la empresa matriz de Facebook, ha identificado en dos ocasiones ejemplos de campañas coordinadas de comportamiento no auténtico en las redes sociales, dirigidas contra defensores y defensoras de los derechos humanos en Marruecos. Según testimonios procedentes de fuentes internas, estas campañas cuentan con la ayuda de comentaristas financiados por el Estado, cuya función es comentar y, por tanto, aumentar la visibilidad de las campañas de desprestigio en Internet.

En muchos casos, estas campañas de desprestigio continuaron después de que las personas defensoras de los derechos humanos fueran encarceladas, puestas en libertad o indultadas, e incluso después de que se marcharan del país.

Marruecos incumple su obligación de respetar el derecho a la privacidad de los defensores y defensoras de los derechos humanos cuando comparte o filtra datos de vigilancia a los medios de comunicación o cuando apoya directamente campañas de desprestigio contra ellos. Además, en virtud del derecho internacional de los derechos humanos, las autoridades marroquíes también deben proteger y hacer efectivos los derechos de los defensores y defensoras de los derechos humanos adoptando medidas para protegerlos de las campañas de desprestigio de agentes privados, y también deben adoptar medidas para hacer efectivos los derechos de los defensores y defensoras creando un entorno seguro y propicio, en el que puedan llevar a cabo su labor.

ACOSO JUDICIAL Y REPRESIÓN

Además de la vigilancia ilícita y las campañas de difamación y desprestigio, los defensores y defensoras de los derechos humanos han sido objeto reiteradamente de procesamiento penal en forma de acusaciones de motivación política, detenciones y encarcelamientos tras juicios sin garantías, o han sido procesados por actos cuya penalización es contraria al derecho internacional.

Muchos de estos juicios han estado empañados por violaciones de los derechos de las personas detenidas y del derecho básico a un juicio con las debidas garantías. Con frecuencia, los defensores y defensoras de los

derechos humanos se han enfrentado a cargos falsos o que criminalizaban sus actividades legítimas, lo que viola el derecho de los derechos humanos. Activistas saharauis y personas activas en el movimiento de protesta Hirak El Rif han sido especialmente señalados por sus actividades de protesta y su activismo, que fueron tratados como delito por “amenazar la seguridad interna del Estado”.

Este informe también documenta casos en los que las autoridades presionaron a defensores y defensoras de los derechos humanos para que prestaran falso testimonio contra compañeros y compañeras suyos.

Aunque algunos de los defensores y defensoras de los derechos humanos que han sufrido esta situación han sido puestos en libertad o indultados, muchos otros continúan privados de libertad.

CONCLUSIÓN

Las organizaciones de derechos humanos llevan decenios documentando la represión contra la sociedad civil en Marruecos. Los profesionales del periodismo y los y las activistas, en particular, trabajan en un entorno muy restringido y se enfrentan a diversas prácticas autoritarias, como la vigilancia ilícita y el acoso judicial, a menudo acompañadas de campañas de desprestigio. Estas tácticas tienen por objeto silenciar la disidencia, atacar la libertad de los medios de comunicación, reducir el espacio de la sociedad civil y afianzar el poder.

Este informe documenta cómo una amplia diversidad de herramientas de vigilancia digital ocupa ahora un lugar central en las prácticas de vigilancia de la DGST, y cómo han permitido a las autoridades marroquíes inmiscuirse en todos los aspectos de la vida de los defensores y defensoras de los derechos humanos. El uso de estas herramientas de vigilancia digital constituye un pilar clave del tecnoautoritarismo, ya que permite a los gobiernos aumentar sus capacidades de control violando los derechos individuales a la privacidad, la reunión pacífica y la libertad de expresión. El impacto humano de estas formas invasivas de vigilancia se pone de manifiesto en los testimonios de las personas defensoras de los derechos humanos entrevistadas para este informe.

El informe también documenta cómo una amplia variedad de actores empresariales han facilitado y posibilitado estas prácticas tecnoautoritarias al seguir suministrando tecnologías de vigilancia digital muy avanzadas a Marruecos, ignorando al mismo tiempo las pruebas de cómo se han utilizado estas herramientas para violar los derechos humanos. Por ejemplo, desde 2017, Amnistía Internacional ha publicado varias investigaciones que documentan la persecución ilícita de la sociedad civil marroquí con el programa espía Pegasus, que continuó al menos hasta noviembre de 2021. NSO Group afirma que el programa espía Pegasus sólo se utiliza para “investigar el terrorismo y la delincuencia”. Numerosas investigaciones realizadas por Amnistía Internacional y otras organizaciones de la sociedad civil de todo el mundo han demostrado que, en realidad, los gobiernos han utilizado reiteradamente el programa espía Pegasus para atacar a defensores y defensoras de los derechos humanos, periodistas y otros miembros de la sociedad civil. Esta investigación demuestra que, al menos en el caso de Marruecos, la sociedad civil no fue una mera víctima ocasional, sino que, en realidad, fue el principal objetivo de la DGST una vez que este organismo adquirió el sistema de software espía, y representó casi dos tercios de los objetivos en los cuatro primeros meses de su funcionamiento. Este informe documenta asimismo que la participación de NSO Group no se limita al momento de la adquisición. El programa espía Pegasus no es utilizado de forma autónoma por los clientes gubernamentales, sino que depende del mantenimiento y la asistencia de NSO Group para seguir funcionando.

La combinación de vigilancia ilícita, acoso judicial y campañas de desprestigio genera un profundo efecto intimidatorio en los defensores y defensoras de los derechos humanos y en la sociedad en general. El uso de la tecnología como arma es fundamental para esta triple amenaza: Al no haber medio de saber cuándo están siendo observadas y grabadas, enfrentándose a riesgos desconocidos para sus familiares y amistades, preocupadas por el escarnio público o incluso por la posibilidad de ir a la cárcel si alzan la voz, muchas personas temen hacerlo, y el espacio para la disidencia se vuelve cada vez más hostil.

Pese a ello, muchas personas siguen alzando la voz e intentando que quienes ejercen el poder rindan cuentas. Sus casos se destacan en este informe. Sus historias subrayan la urgente necesidad de que las autoridades marroquíes pongan fin a la impunidad de que goza la DGST, reformen sus leyes y prácticas y conviertan Marruecos en un espacio seguro para periodistas y defensores y defensoras de los derechos humanos.

Las conclusiones de este informe ponen de manifiesto la inacción de las autoridades marroquíes a la hora de proteger y hacer respetar los derechos humanos básicos de los defensores y defensoras de estos derechos, tal como garantiza el derecho internacional. Este informe también evidencia el papel fundamental

que desempeñan quienes denuncian irregularidades a la hora de sacar a la luz los abusos contra los derechos humanos.

El uso combinado por las autoridades marroquíes de la vigilancia ilícita, el acoso judicial y la represión ha dado lugar a violaciones de numerosos derechos humanos, entre ellos los derechos a la privacidad, a la libertad y a la libertad de expresión, de asociación y de reunión pacífica.

También ha generado un profundo efecto intimidatorio, que causa daños psicológicos, sociales y profesionales a las personas afectadas y disuade a otras y a la sociedad en general de ejercer legítimamente sus derechos humanos.

Amnistía Internacional escribió a las autoridades marroquíes para hacerles llegar un resumen de sus conclusiones un mes antes de la publicación e invitarlas a responder. Las autoridades marroquíes no respondieron.

Antes de la publicación, Amnistía Internacional escribió a las empresas mencionadas en el informe para comunicarles nuestras conclusiones principales relacionadas con sus actividades. Verint respondió que “Verint desinvirtió de esta línea de negocio el 1 de febrero de 2021. Las consultas de los medios de comunicación deben remitirse a Cognyte Software Ltd.” Amnistía Internacional no recibió respuesta de ninguna de las demás empresas.

RECOMENDACIONES CLAVE

A LAS AUTORIDADES MARROQUÍES:

- Poner en libertad a las personas encarceladas en relación con el ejercicio legítimo de sus derechos humanos.
- Poner fin de inmediato a la vigilancia de periodistas y defensores y defensoras de los derechos humanos que ejercen legítimamente sus derechos humanos, y respetar y garantizar su derecho a la privacidad.
- Llevar a cabo las reformas legislativas necesarias para instaurar un marco normativo de derechos humanos que regule la vigilancia y permita prevenir los abusos en la práctica, en especial con respecto a la DGST y otros organismos de seguridad. Hasta que exista un marco de ese tipo, deberá aplicarse una moratoria sobre la compra, venta, transferencia y uso de equipos de vigilancia.
- Garantizar una investigación independiente, efectiva y sistémica sobre la DGST, que incluya todos los casos denunciados de vigilancia ilícita; exigir que todos los responsables rindan cuentas, y proporcionar recursos efectivos a las víctimas, incluidas vías significativas de reparación judicial, por los daños físicos y mentales, así como por la pérdida de medios de vida.
- Poner fin a toda participación de actores estatales en campañas de difamación y desprestigio contra defensores y defensoras de los derechos humanos y periodistas, incluso en las redes sociales, y tomar medidas para proteger a quienes defienden los derechos humanos frente a tales campañas en los medios de comunicación.

A TODOS LOS ESTADOS:

- Denegar la autorización para exportar a Marruecos programas espía, herramientas de análisis forense digital y otras tecnologías que vulneran la privacidad hasta que se haya llevado a cabo una investigación exhaustiva, independiente y efectiva sobre la vigilancia ilícita de periodistas, activistas políticos y defensores y defensoras de los derechos humanos, y se haya instaurado un sistema de salvaguardias de derechos humanos que permita evitar los abusos contra los derechos humanos en la práctica.
- Prohibir a las empresas la producción, venta, transferencia o asistencia de software espía altamente invasivo, cuyas funciones no puedan limitarse y cuyo uso no pueda auditarse de forma independiente.

A LOS ESTADOS DESDE LOS QUE SE EXPORTAN, VENDEN O INTERMEDIAN TECNOLOGÍAS DE VIGILANCIA U OTRAS TECNOLOGÍAS QUE VULNERAN LA PRIVACIDAD:

- Llevar a cabo una investigación sobre la exportación, venta, transferencia o intermediación de tecnología vinculada a los abusos contra los derechos humanos mencionados en este informe, y revocar las licencias de exportación cuando existan pruebas o un riesgo significativo de que estén relacionadas con abusos contra los derechos humanos.
- Impedir que las empresas actúen como intermediarias o faciliten de cualquier otro modo la venta, transferencia o asistencia de tecnologías de vigilancia y otras tecnologías que atenten contra la privacidad a Marruecos hasta que se haya llevado a cabo una investigación exhaustiva, independiente y efectiva sobre la vigilancia ilícita de periodistas, activistas políticos y defensores y defensoras de los derechos humanos, y se haya instaurado un sistema de salvaguardias de derechos humanos que permita evitar en la práctica las violaciones de derechos humanos.

A LAS EMPRESAS IMPLICADAS EN EL SUMINISTRO DE TECNOLOGÍAS DE VIGILANCIA Y OTRAS TECNOLOGÍAS QUE VULNERAN LA PRIVACIDAD A MARRUECOS:

- Suspender toda venta, exportación y transferencia de todo tipo de tecnologías de vigilancia a Marruecos, así como toda intermediación u otra clase de apoyo a tales ventas, transferencias o asistencia, hasta que se haya llevado a cabo una investigación exhaustiva, independiente y efectiva sobre la vigilancia ilícita de periodistas, activistas políticos y defensores y defensoras de los derechos humanos, y se haya instaurado un sistema de salvaguardias de los derechos humanos que permita evitar en la práctica las violaciones de derechos humanos.
- Implantar mecanismos sólidos de reparación, que incluya indemnización para las víctimas de vigilancia ilícita u otras formas de resarcimiento.

A LOS PROVEEDORES DE TELECOMUNICACIONES (MÓVILES O INTERNET) EN MARRUECOS:

- Ejercer una diligencia debida adecuada en materia de derechos humanos con el fin de identificar, prevenir y mitigar los efectos negativos en esos derechos y rendir cuentas por ellos, especialmente en relación con la vigilancia, y, en particular, realizar una evaluación exhaustiva de los riesgos del intercambio ilícito de datos y hacer públicas esas evaluaciones.
- Desarrollar mecanismos de reclamación accesibles y seguros a través de los cuales puedan atenderse de forma efectiva las quejas relativas a las tecnologías de vigilancia y su uso. Estos mecanismos estarán disponibles en todos los países, y deberán adoptarse medidas para garantizar que sean accesibles para todas las personas.

**AMNISTIA 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/AmnestyGlobal



[@Amnesty](https://twitter.com/Amnesty)

“EMPEZAMOS POR LA SENTENCIA”

DENTRO DE LA MAQUINARIA DE VIGILANCIA DE MARRUECOS

RESUMEN EJECUTIVO

Este informe documenta el ecosistema de vigilancia que permite a las autoridades marroquíes utilizar tácticas represivas para acosar, desacreditar y, a la larga, silenciar a los defensores y defensoras de los derechos humanos. El informe describe el papel del servicio de inteligencia nacional de Marruecos, la Dirección General de Vigilancia del Territorio (DGST), en la realización de operaciones de vigilancia contra la sociedad civil. Estas operaciones suelen ir acompañadas de campañas de desprestigio en los medios de comunicación afines al Estado. Las prácticas tecnoautoritarias empleadas por la DGST y documentadas en este informe han sido facilitadas y posibilitadas por diversos actores empresariales. El informe también contiene un análisis exhaustivo del sistema de software espía Pegasus y de cómo lo ha utilizado Marruecos para atacar a defensores y defensoras de los derechos humanos y a periodistas, tanto dentro de Marruecos como a escala internacional.