



“UNA PRISIÓN DIGITAL”

VIGILANCIA Y SUPRESIÓN DE LA SOCIEDAD CIVIL EN SERBIA
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.

© Amnesty International 2020

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.



Foto de portada: *Imagen compuesta creada por Amnistía Internacional a partir de fotografías facilitadas por Sviče y Dragan Gmizic.*

Publicado por primera vez en 2020
por Amnesty International Ltd.
Peter Benenson House, 1 Easton Street
London WC1X 0DW, Reino Unido

Índice: EUR 70/8814/2024 Spanish
Idioma original: Inglés

amnesty.org



RESUMEN EJECUTIVO

En febrero de 2024, Slaviša Milanov, periodista independiente de Dimitrovgrado (Serbia) que cubre noticias de interés local, fue llevado a una comisaría tras un control de tráfico aparentemente rutinario.

Tras ser liberado, Slaviša se dio cuenta de que su teléfono, que había dejado en la recepción de la comisaría a petición de los agentes, funcionaba de un modo extraño: los ajustes de datos y wifi estaban apagados. Como sabía que esto podía ser un indicio de piratería informática, y consciente de las amenazas de vigilancia a las que se enfrentan los profesionales del periodismo en Serbia, Slaviša se puso en contacto con el Laboratorio sobre Seguridad de Amnistía Internacional para solicitar un análisis de su teléfono.

El análisis de Amnistía Internacional llevó a dos descubrimientos importantes. En primer lugar, las huellas forenses revelaron que se había utilizado un producto de Cellebrite para desbloquear el dispositivo. Cellebrite, cuya herramienta de análisis forense permite extraer todos los datos de un dispositivo y que se utiliza en departamentos de policía de todo el mundo, afirma que tiene políticas estrictas para impedir el uso indebido de su producto; sin embargo, este descubrimiento proporciona pruebas claras de que el teléfono de un periodista fue objeto de un ataque sin ningún tipo de garantías procesales. A Slaviša no se le pidió la contraseña de su dispositivo Android ni él la facilitó. Las autoridades no le informaron de que tenían intención de registrar su dispositivo, ni declararon ningún fundamento jurídico que justificara tal registro. Slaviša sigue sin saber qué datos se extrajeron de su teléfono.

El segundo hallazgo del análisis fue aún más extraordinario. Amnistía Internacional encontró rastros de una forma de software espía desconocida hasta entonces, a la que ha denominado “NoviSpy”. NoviSpy permite capturar datos personales sensibles del teléfono del objetivo tras la infección y ofrece la posibilidad de encender el micrófono o la cámara del teléfono a distancia. Las pruebas forenses indican que el programa espía se instaló mientras la policía serbia estaba en posesión del dispositivo de Slaviša, y que la infección dependía del uso de Cellebrite para desbloquear el dispositivo. Se combinaron dos formas de tecnologías altamente invasivas para atacar el dispositivo de un periodista independiente, con lo que casi toda su vida digital quedó a disposición de las autoridades serbias.

La historia no termina con Slaviša. Otras investigaciones de Amnistía Internacional han desvelado la amplitud de la vigilancia digital en Serbia, incluido el despliegue de al menos tres formas diferentes de programas espía, así como el persistente uso indebido de la sofisticadísima tecnología forense digital de Cellebrite.

Este informe es un estudio de caso sobre cómo las autoridades serbias han desplegado la tecnología de vigilancia y las tácticas de represión digital como instrumentos de un control estatal más generalizado y de la represión dirigida contra la sociedad civil. Serbia es un caso paradigmático de un sistema en el que este tipo de herramientas pueden convertirse en facilitadores esenciales de una represión digital, que probablemente se repita en otros países y contextos, y que es muy posible que ya esté ocurriendo.

Este informe se presenta en un momento de intensificación de la represión estatal y en un entorno cada vez más hostil para la libertad de expresión y el debate abierto en el país. En Serbia se han producido varias oleadas importantes de protestas antigubernamentales desde 2021, cada una de las cuales ha desencadenado una respuesta cada vez más dura por parte de las autoridades: desde campañas de difamación sostenidas y despiadadas contra organizaciones no gubernamentales (ONG), medios de comunicación y profesionales del periodismo críticos, hasta el persistente hostigamiento judicial a la ciudadanía que se organiza pacíficamente y participa en la disidencia política.

En este informe, Amnistía Internacional combina extensas entrevistas con representantes de la sociedad civil en Serbia con una investigación forense digital sumamente técnica para sacar a la luz las prácticas

concretas de vigilancia de las autoridades serbias. Al revelar estas tácticas, el informe pretende potenciar los esfuerzos de la sociedad civil para garantizar la rendición de cuentas por la vigilancia ilegítima, a la vez que se eliminan las capas de secretismo y se reduce la asimetría de la información. La opacidad de la vigilancia digital y la percepción de omnipotencia e impunidad pueden impulsar y alentar a un aparato estatal represivo a llevar a cabo estas prácticas, con un efecto devastador para la salud de la sociedad en su conjunto.

Las conclusiones del informe revelan que en Serbia se hace un uso generalizado y rutinario de programas espía invasivos, como el programa espía Pegasus de NSO Group, junto con un novedoso sistema espía para Android, NoviSpy, de producción nacional, que se revela por primera vez en este informe. La Agencia de Información de Seguridad serbia, conocida en el país como la BIA (*Bezbedonosno-informaciona Agencija*) y la policía serbia han utilizado el programa espía NoviSpy, junto con herramientas forenses para móviles de Cellebrite, para perseguir a activistas de grupos consultivos independientes, manifestantes pacíficos y periodistas independientes.

En conjunto, estas herramientas proporcionan al Estado una enorme capacidad para recopilar datos tanto de forma encubierta, como en el caso de los programas espía, como de forma abierta, mediante el uso ilegal e ilegítimo de la tecnología de extracción de Cellebrite para teléfonos móviles. Las autoridades de Serbia han desplegado sistemáticamente estas herramientas contra personas que se manifiestan pacíficamente y que ya son objeto con demasiada frecuencia de criminalización injustificada por su activismo. Esta vigilancia digital y recopilación de datos ilegítimas dirigidas contra la sociedad civil viola el derecho de las personas a la privacidad y a la protección de los datos personales, y afecta profundamente al resto de sus derechos y libertades, incluidos los derechos a la libertad de expresión, de asociación y de reunión pacífica.

Las conclusiones de este informe se basan en entrevistas a fondo con 13 personas directamente afectadas por programas espía o productos de extracción de datos de móviles, u otras formas de vigilancia digital, y con 28 representantes de la sociedad civil de toda Serbia que aportaron una valiosísima perspectiva del entorno cada vez más difícil en el que operan. Sus testimonios fueron corroborados por análisis forenses detallados de los dispositivos móviles de una veintena de activistas y periodistas realizados por el Laboratorio sobre Seguridad de Amnistía Internacional. Dicho laboratorio utilizó herramientas forenses digitales desarrolladas por Amnistía Internacional, como el Mobile Verification Toolkit (MVT) de código abierto y AndroidQF, para reunir y analizar pruebas forenses para este informe.

AMENAZAS DE LOS PROGRAMAS ESPÍA PARA LA SOCIEDAD CIVIL SERBIA

El informe detalla el historial de uso o adquisición de programas espía altamente invasivos, incluidos los sistemas de Finfisher, NSO Group e Intellexa, por parte de las autoridades serbias durante el último decenio.

Un aspecto decisivo de la investigación es que al menos a tres activistas y a un periodista independiente les instalaron de forma encubierta el programa espía NoviSpy en sus dispositivos mientras asistían a entrevistas informativas con la policía serbia o con la BIA. Las infecciones se produjeron cuando los teléfonos se habían retirado temporalmente a sus propietarios y, al parecer, se habían depositado en taquillas de las comisarías. Esta táctica excepcionalmente engañosa, es decir, instalar programas espía de forma encubierta en los dispositivos de las personas durante las entrevistas informativas, parece haber sido ampliamente utilizada. Las pruebas técnicas sugieren que el programa espía NoviSpy se ha utilizado en decenas, si no centenares, de dispositivos durante los últimos años. Es probable que el alcance total de los objetivos vaya más allá de la persecución ilegítima de la sociedad civil.

En octubre de 2024, un activista de la ONG Krokodil, con sede en Belgrado, fue convocado a la oficina de la BIA para facilitar información sobre un incidente relacionado con un ataque a su organización. Durante su asistencia a la reunión, su teléfono quedó desatendido fuera de la sala de entrevistas. Un análisis forense posterior realizado por el Laboratorio sobre Seguridad de Amnistía Internacional encontró pruebas de que durante ese tiempo se había instalado el programa espía NoviSpy para Android. Aunque técnicamente sea un programa menos avanzado que otros programas espía comerciales como Pegasus, el programa espía NoviSpy para Android proporciona a las autoridades serbias amplias capacidades de vigilancia una vez instalado en el dispositivo del objetivo. Además de Slaviša y el activista de Krokodil, Amnistía Internacional encontró indicios de instalación o intento de instalación del programa espía NoviSpy en al menos otros dos casos relacionados con activistas serbios de la sociedad civil.

En respuesta a estos hallazgos, NSO Group, que desarrolló Pegasus, no pudo confirmar si Serbia era su cliente, pero declaró que el Grupo “se toma en serio su responsabilidad de respetar los derechos humanos, y está firmemente comprometido a evitar causar, contribuir o estar directamente vinculado a impactos negativos sobre los derechos humanos, y a revisar exhaustivamente todas las acusaciones creíbles de uso indebido de los productos de NSO Group”.

EL PROGRAMA ESPÍA NOVISPY SE CONECTA A LA BIA

Un análisis de varias muestras de la aplicación espía NoviSpy recuperadas de dispositivos infectados reveló que todas se comunicaban con servidores alojados en Serbia, tanto para recuperar comandos como para vigilar datos. En particular, una de estas muestras del programa espía estaba configurada para conectarse directamente a un rango de direcciones IP asociado directamente con la BIA de Serbia. La investigación también descubrió que los datos de configuración integrados en la muestra de software espía se relacionan con un empleado específico de la BIA, que anteriormente estuvo vinculado a los esfuerzos de Serbia por adquirir software espía para Android de Hacking Team, proveedor de software espía ya desaparecido.

Estos importantes errores operativos de seguridad, y el hecho de que el software espía se instalara en varios casos durante las entrevistas con funcionarios de la BIA, permiten a Amnistía Internacional atribuir con un alto grado de confianza estas campañas de software espía a la BIA y a las autoridades serbias.

USO INDEBIDO DE LAS HERRAMIENTAS DE ANÁLISIS FORENSE DIGITAL DE CELLEBRITE

Este informe también revela el uso generalizado e ilegítimo de la tecnología de extracción Cellebrite para descargar datos personales de los teléfonos de quienes organizan protestas y de periodistas. Los datos obtenidos mediante el uso de estas herramientas pueden permitir a las autoridades cartografiar las redes sociales de los movimientos de protesta, recopilar conversaciones cifradas de aplicaciones como Signal y Telegram, y extraer datos almacenados en la nube. De hecho, la posibilidad de descargar toda la vida digital de una persona mediante Cellebrite UFED y otras herramientas forenses similares para móviles plantea enormes riesgos para los derechos humanos si estas herramientas no están sujetas a un control y una supervisión estrictos. Los controles legales sobre el uso de tales herramientas en Serbia son insuficientes y el uso de productos forenses de Cellebrite por parte de Serbia plantea graves riesgos para los derechos humanos.

Al menos en dos casos documentados por Amnistía Internacional, el producto Cellebrite UFED y el aprovechamiento de vulnerabilidades (*exploits*) asociado se utilizaron para eludir de forma encubierta las funciones de seguridad de los teléfonos, lo que permitió a las autoridades serbias infectar los dispositivos con el programa espía NoviSpy. Estas infecciones encubiertas, que también se produjeron durante entrevistas con la policía o con la BIA, sólo fueron posibles gracias a las capacidades que ofrece una tecnología avanzada como Cellebrite UFED para eludir el cifrado de los dispositivos. Aunque las personas que se dedican al activismo llevan mucho tiempo expresando su preocupación por las infecciones de software espía que se producen durante interrogatorios policiales, Amnistía Internacional cree que este informe describe las primeras infecciones de software espía documentadas desde un punto de vista forense y facilitadas por el uso de la tecnología forense para móviles de Cellebrite.

Esta investigación también descubrió un *exploit* de día cero de escalada de privilegios en Android utilizado en Cellebrite UFED, que fue parcheado en el curso de esta investigación, lo que ayuda a proteger millones de dispositivos Android. En colaboración con especialistas en seguridad de Google, Amnistía Internacional identificó los *exploits* a partir del análisis minucioso de los registros forenses encontrados en el teléfono de una persona que había organizado una protesta y que había sido detenida por las autoridades serbias.

REPRESIÓN DEL ESPACIO CÍVICO EN SERBIA

La vigilancia digital en Serbia tiene lugar en medio de una creciente represión estatal y un clima de deterioro de la libertad de expresión. Desde 2021, en el país se han producido numerosas protestas antigubernamentales, cada una de ellas reprimida con mayor dureza por las autoridades. Tras las protestas masivas que se produjeron en todo el país en julio y agosto de 2024 contra la extracción de litio y el acuerdo de Serbia con la Unión Europea (UE) sobre el acceso a las materias primas, el ataque del gobierno a la sociedad civil se intensificó drásticamente. En agosto, TV Informer, un medio progubernamental de gran audiencia, publicó extensos reportajes en los que sugería que unas 40 ONG “financiadas desde el

“UNA PRISIÓN DIGITAL”

VIGILANCIA Y SUPRESIÓN DE LA SOCIEDAD CIVIL EN SERBIA

Amnistía Internacional

extranjero” estaban “librando una guerra especial contra Serbia” a instancias de donantes extranjeros, calificándolas de “mercenarios extranjeros”. Las declaraciones difamatorias sobre estas organizaciones fueron alimentadas además por altos funcionarios, entre ellos el presidente, miembros del Parlamento y el gobernador del Banco Nacional.

Al mismo tiempo, los/as activistas que participaban en las protestas contra el litio o hablaban de ellas se enfrentaban a detenciones y acusaciones penales infundadas, aunque extremadamente graves, como la de “incitar al derrocamiento violento del orden constitucional”, un delito penal castigado con penas de hasta ocho años de prisión. Activistas y profesionales de la abogacía entrevistados para el informe relataron cómo la policía citaba con frecuencia las publicaciones de activistas en las redes sociales, sus discursos o su mera participación en las protestas como base para estas acusaciones. Según Civic Initiatives, al menos 33 personas fueron detenidas o encarceladas durante las protestas de agosto, sometidas a largos interrogatorios, al registro de sus apartamentos y a la incautación y registro de sus teléfonos y ordenadores. Ninguna de ellas ha sido acusada formalmente en el momento de la publicación de este informe.

Amnistía Internacional habló con nueve activistas a quienes se detuvo o interrogó entre julio y noviembre de 2024 y cuyos teléfonos y ordenadores fueron incautados temporalmente por la policía y sometidos a registros exhaustivos, incluida la extracción de datos digitales para que los fiscales pudieran decidir si presentaban cargos formales contra sus personas o no. Sin embargo, los/as activistas sospechaban que estas medidas de investigación intrusivas, que al parecer son legales según la legislación serbia, eran un pretexto de la policía y los servicios de seguridad para conocer mejor sus redes sociales y sus planes de futuro, más que para presentar cargos penales.

EL INADECUADO MARCO JURÍDICO Y DE SUPERVISIÓN DE LA VIGILANCIA DIGITAL EN SERBIA

La legislación de Serbia prevé el uso de medidas excepcionales, incluida la vigilancia secreta de las comunicaciones, y establece circunstancias específicas en las que dichas medidas podrían utilizarse legalmente. Sin embargo, el despliegue de tecnologías avanzadas, incluidos programas espía y otras herramientas forenses digitales avanzadas que recopilan grandes cantidades de datos personales, no está plenamente reconocido ni suficientemente regulado por la ley, lo que deja demasiado espacio para posibles abusos de tales técnicas, incluso con fines políticos.

Las disposiciones genéricas que regulan la aplicación de medidas especiales en varias leyes diferentes no son suficientemente claras, ni proporcionan salvaguardias significativas contra el uso indebido cuando se trata de tecnologías de vigilancia digital, que son mucho más intrusivas y menos selectivas que los medios convencionales de vigilancia encubierta de las comunicaciones, como las escuchas telefónicas. Ni siquiera el mecanismo de supervisión judicial previa —como una decisión judicial que especifique las medidas, los plazos estrictos y el objetivo de una vigilancia— puede proporcionar una protección eficaz contra las herramientas avanzadas de vigilancia digital, especialmente los programas espía, que pueden obtener un acceso completo e incontrolado a los datos, mensajes, imágenes, archivos y metadatos del dispositivo de una persona.

Además, en el contexto de los motivos de preocupación que frecuentemente se vienen expresando sobre la indebida influencia política del gobierno en tribunales y fiscales y sobre el grado de control del Estado en Serbia, los medios de fiscalización y supervisión del uso de medidas especiales, que en teoría podrían parecer suficientes, en la práctica pierden sentido o son ineficaces.

El gobierno serbio no hizo comentarios sobre las conclusiones del informe, cuyos detalles se les comunicaron antes de su publicación.

EFFECTO DISUASORIO

La vigilancia digital no sólo tiene un efecto devastador sobre el derecho de las personas a la privacidad, sino que también afecta profundamente a los derechos a la libertad de expresión, de asociación y de reunión pacífica. Activistas de Serbia contaron a Amnistía Internacional que al enterarse de que eran objeto de vigilancia las personas se sintieron violadas, vulnerables y solas, y se vieron obligadas a reconsiderar o cambiar su comportamiento. Algunas se volvieron más reacias a hablar sobre temas controvertidos, mientras que otras decidieron volverse más discretas o desvincularse por completo del activismo.

Tras enterarse de que había sido objeto de ataques, a Slaviša le preocupaba mucho que algunas de sus fuentes pudieran haber estado en peligro y tuvo que cambiar la forma en que investigaba sus artículos y se relacionaba con las fuentes:

“Ya no puedo utilizar el teléfono ni el correo electrónico y tengo que buscar otras formas de hablar con la gente, incluso en persona. Tiendo a hacerlo sólo cuando estamos en lugares públicos y en grupos grandes, lo que obviamente no es lo ideal”.

“Goran” fue otro de los activistas atacados con Pegasus y entrevistado por Amnistía Internacional. Para él, el ataque supuso un gran examen de conciencia sobre su futuro trabajo.

“Me llevó a cuestionar mi compromiso con la organización. Me pregunté si debía seguir trabajando y cómo afectaba esto a la organización, y me planteé retirarme. Un ataque de este tipo realmente socava la integridad personal y la actitud hacia el trabajo, y te hace cuestionarte si a pesar de todo estás dispuesto a seguir haciendo lo que haces. Tenía cientos de preguntas”.

“Goran” se quedó en la organización, pero tuvo que introducir numerosas medidas de seguridad tanto en su vida personal como en su organización.

“Si el gobierno puede hacer lo que me hizo a mí, el próximo objetivo puede ser otra persona. Me di cuenta de que las actividades de todas las organizaciones de la sociedad civil están sometidas a un escrutinio constante por parte de las autoridades y que debemos permanecer vigilantes”.

Para las organizaciones que ya se enfrentaban a numerosas presiones, tener que lidiar con cuestiones de seguridad digital suponía una distracción más a la hora de realizar su trabajo principal, dijo un activista de Krokodil a Amnistía Internacional:

“Tener que hacer frente a tantos ataques diferentes al mismo tiempo nos mantiene muy ocupados y nos debilitará de manera muy profunda, hasta el punto de que no podremos operar en absoluto... Éste es probablemente el objetivo”.

RESPONSABILIDADES DE LAS EMPRESAS Y OTRAS PARTES EN MATERIA DE DERECHOS HUMANOS

Aunque los Estados tienen el deber primordial de cumplir el derecho internacional de los derechos humanos, las empresas y otras partes tienen la responsabilidad de respetar los derechos humanos en cualquier lugar del mundo en el que operen y en todas sus actividades empresariales. Una parte fundamental del cumplimiento de esta responsabilidad es la aplicación adecuada de la diligencia debida en materia de derechos humanos para identificar, prevenir y mitigar los posibles riesgos para tales derechos a los que puedan contribuir las empresas. Amnistía Internacional ha descubierto que varias empresas han incumplido sus responsabilidades en materia de derechos humanos en Serbia.

Además, el Ministerio de Asuntos Exteriores noruego (que donó la tecnología Cellebrite UFED) y la Oficina de las Naciones Unidas de Servicios para Proyectos (UNOPS, que gestionó la concesión de la subvención del gobierno noruego al Ministerio del Interior serbio) no llevaron a cabo un proceso adecuado de diligencia debida para evaluar y mitigar los posibles riesgos de esta tecnología para los derechos humanos ni proporcionaron salvaguardias contra su uso indebido. Dada la debilidad del marco regulador de la vigilancia digital en Serbia, la preocupación por la independencia del poder judicial y los informes persistentes de amenazas a la sociedad civil y a periodistas independientes, el gobierno noruego y la Oficina de las Naciones Unidas de Servicios para Proyectos tenían la responsabilidad de ejercer la supervisión y la diligencia debida al adquirir tecnología altamente invasiva y entregarla a instituciones serbias. Al no haberlo hecho, permitieron y contribuyeron a las violaciones por parte de Serbia de los derechos de las personas a la privacidad, la libertad de expresión, de asociación y de reunión pacífica mediante la vigilancia digital ilegítima.

En una respuesta a los detalles de los hallazgos, el Ministerio de Asuntos Exteriores noruego afirmó que “el Ministerio considera alarmante que las herramientas forenses digitales, adquiridas a través de un proyecto financiado por Noruega, puedan haber sido utilizadas indebidamente para atacar a miembros de la sociedad civil en Serbia”, y añadió que, “de ser cierto, [esto] supondría una clara violación de los principios básicos de la ayuda noruega al desarrollo, y del propósito acordado del apoyo a las autoridades serbias en aquel momento”. El Ministerio añadió que se espera que UNOPS, que era responsable de todas las actividades del proyecto, lleve a cabo una investigación exhaustiva del presunto uso indebido.

“UNA PRISIÓN DIGITAL”

VIGILANCIA Y SUPRESIÓN DE LA SOCIEDAD CIVIL EN SERBIA

Amnistía Internacional

Otro aspecto igualmente crucial es que Cellebrite tenía la responsabilidad de llevar a cabo la diligencia debida en materia de derechos humanos para garantizar que su producto no causaba ni contribuía a causar impactos adversos sobre los derechos humanos. En su sitio web, Cellebrite afirma que la empresa “tomará todas las medidas necesarias para prohibir que agentes malintencionados utilicen o tengan acceso” a sus soluciones cuando la tecnología de Cellebrite “se utilice sin atenerse al derecho internacional, no cumpla las condiciones de uso de Cellebrite o no esté en consonancia con los valores corporativos de Cellebrite”. Sin embargo, toda la información disponible hasta la fecha indica que Cellebrite no ha tomado medidas suficientes y efectivas para utilizar su influencia para abordar los riesgos que existen para los derechos humanos en Serbia. Como demuestra la investigación de Amnistía Internacional en Serbia, el uso del producto de Cellebrite ha tenido un impacto adverso en los derechos humanos de activistas y periodistas de ese país. Como mínimo, Cellebrite guarda relación directa con estas violaciones de los derechos humanos.

Cellebrite no ha cumplido con su responsabilidad empresarial en virtud de los Principios rectores de la ONU sobre las empresas y los derechos humanos con el fin de mitigar y prevenir los daños potenciales y reales a los defensores y defensoras de los derechos humanos y, por lo tanto, se necesitan políticas y procedimientos más eficaces de diligencia debida en materia de derechos humanos. En situaciones en las que una empresa ha contribuido a causar impactos reales, la empresa también debe proporcionar reparación a las personas afectadas.

Respondiendo a las preguntas que Amnistía Internacional envió durante el proceso de investigación, tal como se explica con más detalle en el informe completo, Cellebrite envió una breve respuesta en la que afirmaba que no era una empresa de vigilancia y que no proporcionaba tecnología de cibervigilancia ni programas espía. Señaló que el producto de la empresa era una “plataforma de investigación digital [que] equipa a organismos encargados de hacer cumplir la ley con la tecnología necesaria para proteger y salvar vidas, acelerar la justicia y preservar la privacidad de los datos”, y que sus productos “tienen licencia estrictamente para uso legal, requieren una orden judicial o consentimiento para ayudar a los organismos encargados de hacer cumplir la ley con investigaciones legalmente sancionadas después de que se haya producido un delito”.

Antes de su publicación, Amnistía Internacional compartió las conclusiones de este informe con Cellebrite. Cellebrite, en respuesta a estas comunicaciones, ha manifestado: “Nuestras soluciones de software de investigación digital no instalan malware ni realizan vigilancia en tiempo real consistente con spyware o cualquier otro tipo de actividad cibernética de carácter ofensivo”.

“Agradecemos a Amnistía Internacional que haya señalado el presunto uso indebido de nuestra tecnología. Nos tomamos muy en serio todas las denuncias sobre posible uso indebido de nuestra tecnología por parte de un cliente en formas que pudieran contravenir las condiciones explícitas e implícitas recogidas en nuestro acuerdo de usuario final.

“Estamos investigando las afirmaciones que se realizan en este informe. En caso de confirmarse, estamos dispuestos a imponer las sanciones correspondientes, incluida la terminación de la relación de Cellebrite con cualquier entidad pertinente.”

El análisis completo de las responsabilidades de la empresa en materia de derechos humanos puede consultarse en el informe completo y las dos respuestas de la empresa pueden encontrarse en el apéndice del informe.

CONCLUSIÓN Y RECOMENDACIONES

Las conclusiones de este informe son emblemáticas y muestran cómo un aparato estatal represivo puede combinar prácticas de vigilancia dispares para lograr sus objetivos. El informe también destaca las nuevas tácticas de vigilancia, como el uso generalizado de herramientas forenses digitales invasivas para recopilar datos de personas que se manifestaron pacíficamente y no estaban acusadas de ningún delito. A medida que las mejoras en la seguridad hacen que los ataques de *0 clics* y de otros programas espía remotos resulten prohibitivamente caros o inviábiles, las autoridades pueden recurrir cada vez más a infectar los dispositivos con programas espía mediante el acceso físico a un dispositivo. De hecho, algunos Estados han propuesto legislación específica para permitir el allanamiento secreto de domicilios con el fin de infectar dispositivos con programas espía selectivos.

Serbia debe comprometerse a dejar de utilizar inmediatamente programas espía altamente invasivos y a llevar a cabo investigaciones rápidas, independientes e imparciales de todos los casos documentados y denunciados de vigilancia digital ilegítima. También debe tomar medidas concretas para garantizar que las tecnologías digitales no se utilizan indebidamente para violar los derechos humanos, por ejemplo

estableciendo y aplicando firmemente un marco jurídico que proporcione garantías procesales significativas, sistemas efectivos de control y supervisión mediante revisión judicial y mecanismos efectivos de reparación para las víctimas.

Cellebrite y otras empresas de análisis forense digital que diseñan y proporcionan tecnologías altamente intrusivas a las fuerzas del orden y a los organismos de seguridad deben llevar a cabo una diligencia debida significativa y exhaustiva para garantizar que sus productos no se utilizan de un modo que contribuya a la comisión de violaciones de los derechos humanos. En particular, Cellebrite debe investigar cómo se ha utilizado su tecnología en Serbia para evaluar el posible impacto adverso sobre los derechos humanos y actuar de acuerdo con su compromiso de “tomar todas las medidas necesarias”, incluida la no renovación de las licencias de Cellebrite, con objeto de prohibir a los agentes malintencionados que utilicen o tengan acceso a sus soluciones de un modo que resulte incompatible con el derecho internacional.

Véase la lista completa de recomendaciones al final del informe.

**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



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

“UNA PRISIÓN DIGITAL”

VIGILANCIA Y SUPRESIÓN DE LA SOCIEDAD CIVIL EN SERBIA

RESUMEN EJECUTIVO

Este informe documenta cómo las autoridades serbias han desplegado tecnología de vigilancia y tácticas de represión digital como instrumentos de un control estatal más amplio y de represión dirigida contra la sociedad civil. Las conclusiones del informe revelan que en Serbia se hace un uso generalizado y rutinario de programas espía invasivos, como el programa espía Pegasus de NSO Group, junto con un novedoso sistema espía para Android, NoviSpy, de producción nacional, que se revela por primera vez en este informe. El informe destaca el uso indebido y generalizado de las herramientas forenses para móviles UFED de Cellebrite contra activistas ambientales y líderes y lideresas de protestas serbios.