PEGASUS: DENUNCIAS DE VIGILANCIA MASIVA EN ESPAÑA.

10 MEDIDAS QUE GARANTICEN LA NO REPETICIÓN DE VIOLACIONES DE DERECHOS HUMANOS.

25 DE MAYO DE 2022

AMNISTÍA INTERNACIONAL

Publicado por primera vez en 2022
por Amnistía Internacional España.
Calle Fernando VI, 8, 28004 Madrid

es.amnesty.org

PEGASUS: DENUNCIAS DE VIGILANCIA MASIVA EN ESPAÑA - 10 MEDIDAS QUE GARANTICEN LA NO REPETICIÓN DE VIOLACIONES DE DERECHOS HUMANOS.

CONTENIDO

INTRODUCCIÓN

Amnistía Internacional ha advertido de las amenazas de la vigilancia digital y masiva, y su grave impacto en los derechos humanos. La vigilancia de las comunicaciones puede suponer una interferencia en un amplio rango de derechos humanos, en particular el derecho a la privacidad y el derecho a la libertad de expresión y asociación.

El comercio y utilización del software espía llamado Pegasus, desarrollado por la empresa israelí NSO Group, ha puesto sobre la palestra tanto la impunidad de los estados y de las compañías privadas en la utilización de este sistema de vigilancia, como los fallos de los estados en su obligación de proteger a las personas frente a la vigilancia ilícita, también en España. Tras la denuncia por parte de Citizen Lab el pasado 18 de abril sobre la infección con Pegasus de al menos 65 dispositivos de personas pertenecientes al entorno independentista catalán y en parte vasco, entre 2015 y 2020, el 3 de mayo el Gobierno admitía que el teléfono del Presidente del Gobierno y el de la Ministra de Defensa habían sufrido un robo de información con ese mismo software espía entre mayo y junio de 2021, hechos que están siendo investigados en la Audiencia Nacional, donde el juez instructor ha decretado el secreto de la causa. El 10 de mayo, confirmaban también que el teléfono del Ministro de Interior había sido infectado y sufrido un robo de información en el mes de julio de 2021, al que también se sumaba el espionaje del teléfono del Ministro de Agricultura. Ambos casos también han sido incorporados en la investigación que se está llevando a cabo en la Audiencia Nacional.

Aunque NSO Group ha justificado la utilización de este software para la consecución de un fin legítimo - lucha contra el terrorismo y crimen organizado- lo cierto es que las investigaciones de Amnistía Internacional y otras organizaciones han demostrado como ha sido utilizado para la comisión de violaciones de derechos humanos. Por su propia naturaleza este instrumento de vigilancia no tiene límites, ya que está diseñado para realizar una severa injerencia en la privacidad de las personas. Sin una adecuada supervisión, salvaguardas y transparencia, los daños de la vigilancia ilícita son enormes.[1]

1 Amnistía Internacional: Uncorvering the Iceberg. The digital surveillance crisis wrought by States and the private sector. AI index: DOC 10/

1. LAS DENUNCIAS DEL PRESUNTO ESPIONAJE DE LÍDERES CATALANES POR AUTORIDADES ESPAÑOLAS

El pasado 18 de abril, Citizen Lab, un laboratorio perteneciente a la Universidad de Toronto, revelaba que los ordenadores y teléfonos móviles de al menos 65 personas, en su mayoría del entorno independentista catalán habían sido infectados con el programa Candiru los primeros, y el programa Pegasus en el caso de los segundos, un software que según indica la empresa propietaria del mismo, solo se vende a gobiernos y agencias estatales. Entre las 65 personas se encuentran europarlamentarios, representantes políticos, miembros de la sociedad civil y también sus familiares y abogados.[2] Amnistía Internacional ha corroborado esta información mediante la colaboración con Citizen Lab y la revisión independiente de los teléfonos de Elisenda Paluzie, presidenta de la ANC; Sònia Urpí también de la ANC; Jordi Sánchez, expresidente de la ANC o Txell Bonet, mujer del presidente de Òmnium cultural, Jordi Cuixart.[3]

Simultáneamente, el 19 de marzo una Comisión de Investigación del Parlamento Europeo inició los trabajos sobre las infracciones de la legislación de la Unión Europea asociadas al uso de Pegasus y otros programas equivalentes. Amnistía Internacional criticaba en una comparecencia ante esa comisión que las instituciones de la Unión Europea estaban incumpliendo su deber de poner fin a las violaciones de derechos humanos generalizadas cometidas con software espía. También Instaba a no dejar piedra sin remover al documentar las violaciones de derechos humanos facilitadas por programas espía ilegales; eso incluye investigar estas nuevas revelaciones"[4]

La denuncia de la infección de los teléfonos y posible espionaje de figuras relevantes del independentismo catalán no es nueva. En mayo de 2019 una vulnerabilidad de seguridad en la aplicación de mensajería Whatsapp se utilizó para intentar atacar los teléfonos de al menos 1.400 usuarios,[5] entre los cuales se encontraban Roger Torrent, expresidente del Parlament catalán y Ernest Maragall, diputado autonómico del grupo parlamentario ERC. En declaraciones públicas, el Sr. Torrent señaló directamente al gobierno español interponiendo una querella en julio de 2020.

Tanto el Partido Socialista, como el PP y VOX votaron en contra a la apertura de una comisión de investigación por el Caso Pegasus solicitada el 3 de mayo por Podemos, ERC, PNV y Más País. El Gobierno español indicó públicamente que iba a tomar tres medidas: una investigación interna realizada por el propio CNI, otra a realizar por el Defensor del Pueblo, que finalmente abrió una investigación de oficio, y cuyo resultado se hizo público el pasado 18 de mayo, considerando que el espionaje llevado a cabo por el CNI se hizo conforme a la ley, si bien observó deficiencias en relación al control judicial; finalmente la convocatoria de la Comisión de Control de Créditos destinados a Gastos Reservados – comúnmente denominada Comisión de Secretos Oficiales- con la comparecencia en la misma de la entonces Directora, Paz Esteban, posteriormente cesada de su cargo por el gobierno.

2 https://catalonia.citizenlab.ca/es/

3 https://www.amnesty.org/es/latest/news/2022/04/spain-pegasus-spyware-catalans-targeted/

4 Ibid.

5 https://www.amnesty.org/es/latest/research/2019/10/nso-group-tools-abused-whatsapp-to-target-human-rights-defenders-with-invasive-spyware/

2. LA FALTA DE TRANSPARENCIA DEL GOBIERNO ESPAÑOL A LA HORA DE DAR EXPLICACIONES SOBRE LA COMPRA Y USO DE PEGASUS

Tras la denuncia de Citizen Lab y Amnistía Internacional, y dada la gravedad de las informaciones, varios grupos parlamentarios elevaron preguntas al gobierno exigiendo transparencia en sus explicaciones. El 5 de mayo de 2022, durante la comparecencia de la Ministra de Defensa en la Comisión de Defensa, varios grupos parlamentarios preguntaron expresamente sobre la veracidad de las informaciones que apuntarían a que el Gobierno español – y concretamente el Centro Nacional de Inteligencia (CNI)- podría haber utilizado el software espía Pegasus.

La Ministra de Defensa no aclaró si el gobierno español o el CNI habían adquirido o utilizado este programa. Se negó a dar explicaciones sobre las actuaciones del CNI amparándose en la obligación de mantener en secreto sus actuaciones. Tampoco el Ministro de la Presidencia aclaró este punto cuando en una rueda de prensa el 2 de mayo anunció que los teléfonos del Presidente del Gobierno y de la Ministra de Defensa habían sido infectados por el programa Pegasus entre mayo y junio de 2021. Tampoco el Presidente del Gobierno respondió a esta pregunta durante la sesión de control de gobierno celebrada el 11 de mayo.

El 6 de mayo en su comparecencia en la Comisión de Secretos Oficiales, la directora del CNI admitió el espionaje de 18 personas del entorno catalán, entre las que se encontraría el actual President de la Generalitat. Según la información que ha transcendido, la directora del CNI habría mostrado documentación que respaldaría que la intervención de las comunicaciones se habría realizado acorde a la legislación vigente. Sin embargo dado el carácter secreto de lo hablado en dicha comisión, la opinión pública española sigue sin saber si el gobierno español ha realizado algún contrato de compraventa con NSO Group y concretamente si ha adquirido y usado para este fin el programa espía Pegasus, y las personas perjudicadas siguen sin saber cuál ha sido el alcance y consecuencias de la interceptación de sus comunicaciones.

Amnistía Internacional lleva meses pidiendo al gobierno español transparencia y explicaciones sobre la adquisición y uso de Pegasus. En septiembre de 2020 Amnistía Internacional se dirigió por escrito al Ministerio del Interior y pidió información sobre la adquisición de Pegasus, y preguntó si se había abierto algún tipo de investigación interna en relación al posible espionaje de los teléfonos de Torrent y Maragall.[6] Si bien este Ministerio no contestó directamente a la organización, en su comparecencia en la Comisión de Interior del Senado celebrada el 5 de noviembre de 2020, el Secretario de Estado de Seguridad negó que ese Ministerio hubiese hecho uso de este programa o contratado con la empresa NSO.[7] Amnistía Internacional se dirigió al CNI mediante el portal de transparencia para solicitar la misma información. Su respuesta se limitaba a indicar que las actividades del CNI eran constitutivas de información clasificada.

6 Carta enviada al Ministerio del Interior en octubre de 2020.

7 DS. Senado, Comisiones, núm 102, de 5/11/2020

Finalmente, Amnistía Internacional se dirigió por carta al Ministro de la Presidencia en octubre de 2021, donde además de hacerle llegar las últimas investigaciones e informes de la organización denunciando el impacto en derechos humanos de la vigilancia en general, reiterábamos la petición de información sobre los contratos que pudiera tener el gobierno español con la empresa NSO, así como sobre las investigaciones llevadas a cabo por el gobierno ante la querella presentada por el señor Torrent. Estas solicitudes de información, que no han sido aún contestadas, han sido nuevamente reiteradas en abril de 2022 ante las nuevas publicaciones de Citizen Lab y Amnistía Internacional.

3. LOS LÍMITES Y LAS GARANTÍAS DE LA INTERVENCIÓN DE LAS COMUNICACIONES

La privacidad es un derecho humano. El artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos establecen que nadie será objeto de injerencias arbitrarias en su vida privada, su domicilio o su correspondencia, ni de ataques contra su honra y su reputación. Toda persona tiene derecho a la protección de la ley contra estos ataques. Ambos instrumentos internacionales, en su artículo 19, también protegen el derecho de todas las personas a tener sus propias opiniones y a buscar, recibir o difundir información e ideas de toda índole, que puede estar sujeto a ciertas restricciones pero que deben estar expresamente fijadas por la ley y ser necesarias para la protección de la seguridad nacional, el orden público o la salud o la moral públicas. El artículo 8 del Convenio Europeo de Derechos Humanos reconoce el derecho de toda persona a su vida privada y familiar, de su domicilio y de su correspondencia. Su apartado 2 explicita que cualquier injerencia por la autoridad pública deberá estar prevista por la ley, y debe además ser una medida que en una sociedad democrática, sea necesaria para unos fines específicos.[8]

El derecho a la privacidad y al secreto de las comunicaciones también está reconocido en el artículo 18 de la Constitución Española.

Los instrumentos internacionales de derechos humanos reconocen que el derecho a la privacidad no es un derecho absoluto, y puede ser limitado en interés de un fin legítimo. Sin embargo cualquier injerencia por parte de las autoridades debe cumplir un triple test: estar permitida por la ley y ser estrictamente necesaria y proporcionada para la consecución de un interés legítimo. Incluso cuando el fin que se persigue es legítimo, los órganos de inteligencia deben respetar igualmente el derecho internacional de los derechos humanos.[9]

La ley debe ser lo suficientemente clara para dar una adecuada indicación de las condiciones y circunstancias sobre las cuales las autoridades pueden intervenir comunicaciones, debe detallar suficientemente la extensión y el alcance, los motivos para su autorización, quien realiza la intervención, cómo se realiza, cómo debe ser autorizada, así como indicar cualquier discrecionalidad otorgada para la autorización o implementación de las medidas de vigilancia adoptadas. Igualmente, la norma debe contener salvaguardas efectivas para impedir el abuso, como es la supervisión y el acceso a remedios efectivos para los afectados.

El principio de proporcionalidad requiere además que la interferencia sea lo menos intrusiva posible para alcanzar ese fin legítimo. Los principios de necesidad y de proporcionalidad solo se observan cuando existen garantías adecuadas y efectivas para evitar el uso arbitrario. Esto se alcanza no solo con control judicial previo, sino también con revisión de la legalidad continuada y continua, incluyendo también lo

8 Art. 8.2: No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

9 A/HRC/14/46 y A/69/397

relativo al almacenamiento de la información obtenida, con sistemas sólidos e independientes de supervisión, en particular por el poder judicial, ofreciendo a las personas afectadas recursos efectivos en caso de abuso, y cuando sea posible, una notificación de que fueron objeto de medidas de vigilancia o que sus datos han quedado comprometidos.

La vigilancia masiva realizada con programas como Pegasus difícilmente puede cumplir con este criterio. La vigilancia indiscriminada nunca es proporcionada y necesariamente interfiere de manera ilegítima en el derecho a la privacidad y la libertad expresión.

Amnistía Internacional tiene serias dudas sobre si Pegasus puede constituir una injerencia permisible en el derecho de privacidad ya que cuando infecta un teléfono tiene capacidad de recopilar una ilimitada selección de datos privados y personales. Cualquier tipo de información que haya en el aparato infectado es accesible, incluida aquella más sensible que puede ser luego utilizada en su contra sin ninguna notificación subsecuente o posibilidad de impugnar esa vigilancia. Es un programa que no solamente espía objetivos concretos, sino que es fácilmente extensible a su entorno, colaboradores u otras personas del entorno laboral, familiares, etc, con un efecto completamente devastador en lo que se refiere al derecho a la privacidad también de terceros.

La debilidad de los marcos regulatorios para impedir el abuso ha llevado a que el Relator Especial sobre la promoción y protección del derecho a la libertad de expresión y opinión solicite una moratoria inmediata sobre la venta y la transferencia mundial de instrumentos de vigilancia hasta que se establezcan legislación y marco jurídico que pueda garantizar que los gobiernos y agentes no estatales no van a utilizar estos instrumentos de modo ilegítimo.[10]

LA NORMATIVA ESPAÑOLA QUE HA PERMITIDO ESTA VIGILANCIA NO GARANTIZA EL CUMPLIMIENTO DE LOS ESTÁNDARES INTERNACIONALES, NI EL DERECHO A UN RECURSO EFECTIVO.

Durante su comparecencia el pasado 5 de mayo, la Ministra de Defensa criticó las insinuaciones y acusaciones de espionaje contra el CNI alegando además que este organismo "no puede defenderse"[11] y animando a que aquellos que se considerasen víctimas de un delito acudiesen a los tribunales, eso sí, a la vez que reconocía que las actuaciones del CNI son secretas.

La información producida por el CNI está clasificada y protegida bajo la Ley de Secretos Oficiales. El artículo 5.1 de la Ley 11/2002[12], reguladora del Centro Nacional de Inteligencia, establece que *(....) las informaciones o datos que puedan conducir al conocimiento de las anteriores materias, constituyen información clasificada, con el grado de secreto, de acuerdo con lo dispuesto en la legislación reguladora de los secretos oficiales (.....)*. Según lo dispuesto en su artículo 2.2 "*Sin perjuicio de la protección de sus actividades, la actuación del Centro Nacional de Inteligencia será sometida a control parlamentario y judicial en los términos que esta Ley y la Ley Orgánica reguladora del control judicial previo del Centro Nacional de Inteligencia determinan"*.

El artículo 12 relativo al control judicial previo remite a la Ley 2/2002[13] cuyo único artículo designa a un Magistrado del Tribunal Supremo esta responsabilidad, por la cual y mediante resolución motivada deberá *autorizar la adopción de medidas que afecten a la inviolabilidad del domicilio y al secreto de las comunicaciones, siempre que tales medidas resulten necesarias para el cumplimiento de las funciones*

10 La vigilancia y los derechos humanos. A/HRC/41/35, 28 de mayo de 2019

11 Ut supra

12 «BOE» núm. 109, de 07/05/2002.

13 BOE» núm. 109, de 7 de mayo de 2002, páginas 16439 a 16440

asignadas al Centro. La solicitud de autorización deberá hacerse por escrito y contener la especificación de las medidas que se solicitan, hechos en los que basa la solicitud, identificación de las personas afectadas y duración de las medidas solicitadas. Aunque no podrán exceder un plazo de 24 horas en el caso de afección a la inviolabilidad del domicilio o tres meses en el caso de intervención o interceptación de comunicaciones, los plazos pueden ser prorrogados por periodos sucesivos en caso de necesidad por el mismo magistrado.

Esta actividad de control previo judicial también está sometida a secreto. En cuanto al tratamiento de los datos, la ley recoge que será el Secretario de Estado Director del CNI quien ordenará la inmediata destrucción del material relativo a todas aquellas informaciones que, obtenidas mediante la autorización prevista en este artículo, no guarden relación con el objeto de la misma. Es decir, el control de la información recabada por el CNI queda en manos de la misma agencia.

Finalmente, la clasificación de información pública está regulada por la Ley 9/1968, de 5 de abril, de Secretos Oficiales, una ley aprobada durante el régimen franquista y cuya reforma se hizo antes de la promulgación de la Constitución de 1978. Amnistía Internacional ha denunciado en repetidas ocasiones que la Ley de Secretos Oficiales es un obstáculo para la investigación de graves violaciones de derechos humanos y para garantizar el derecho de las víctimas a verdad, justicia y reparación y garantías de no repetición solicitando que la misma sea modificada respetando los estándares internacionales relativos al derecho a información.[14]

LA DEBILIDAD DEL CONTROL DE LAS ACTUACIONES DEL CNI AFECTA AL DERECHO A UN RECURSO EFECTIVO EN CASO DE ABUSO O ACTUACIÓN ILEGÍTIMA.

Basta una rápida lectura de la normativa vigente en relación a las actuaciones del CNI para considerar que la misma no recoge suficientes salvaguardas para que, tal y como establecen los estándares internacionales, pueda haber un adecuado control de la actividad de los servicios de inteligencia y garantizar tanto una revisión de la legalidad continuada y continua en los procedimientos, así como un control judicial adecuado, incluyendo también lo relativo al almacenamiento de la información obtenida, con sistemas sólidos e independientes de supervisión, para evitar actuaciones arbitrarias o abusivas.

Por otro lado, Amnistía Internacional considera que la Comisión de Secretos Oficiales, que hasta la crisis de Pegasus llevaba dos años sin ser constituida, se caracteriza por su secretismo y oscurantismo y no es el lugar adecuado para investigar supuestas violaciones de derechos humanos.[15]

En el año 2015 se operaba una reforma en la Ley de Enjuiciamiento Criminal[16] en todo lo relativo a la interceptación de comunicaciones para dotarlo de mayores garantías, incluyendo la obligación del juez de instrucción de notificar a las personas intervinientes en las comunicaciones interceptadas así como a terceros afectados, incluso cuando los investigados hayan finalmente adquirido la condición de parte procesal o se

14 Amnistía Internacional: ¿Abrimos ya el candado de la Ley de Secretos Oficiales? Preocupaciones y recomendaciones de Amnistía Internacional para la tramitación de la reforma de la Ley 9/1968, de 5 de abril, sobre secretos oficiales.

15 https://www.es.amnesty.org/en-que-estamos/noticias/noticia/articulo/pegasus-la-comision-de-secretos-oficiales-no-es-el-lugar-apropiado-para-investigar-supuestas-violaciones-de-derechos-humanos/

16 Capítulo IV Disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de las comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos. (arts 588 bis a. – 588 bis k) Capítulo V La interceptación de las comunicaciones telefónicas y telemáticas (arts. 588 ter b – 588 ter m) Capítulo VI Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos (arts 588 quater a -588 quater e) Capítulo VII Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización (arts. 588 quinquies a – 588 quinquies c) Capítulo VIII Registro de dispositivos de almacenamiento masivo de información (art. 588 sexies a –art. 588 sexies c) Capítulo IX Registros remotos sobre equipos informáticos (arts. 588 setpies a – 588 septies c) Capítulo X Medidas de aseguramiento (arts. 588 octies)

haya sobreseído el procedimiento[17], y sin embargo estas garantías no afectan a las investigaciones realizadas por el CNI. El Tribunal Supremo, en una sentencia de diciembre de 2010[18] consideraba que al no tener el CNI actividades enmarcadas a perseguir un ilícito penal, los actos generados no pueden ser considerados como actos de prueba y por lo tanto no se rigen por las mismas reglas procesales, considerando que la figura del juez de control no puede ser considerada como la de un anticipado coadyuvante del Juez de Instrucción. En relación a la transparencia y el derecho de la persona afectada a poder acceder a la información completa del expediente, la sentencia considera que siendo necesario que existan mecanismos de desclasificación de la información, no existe un derecho fundamental a la desclasificación de toda materia reservada.

La consideración automática de secreto de todas las actividades del CNI y la falta de control posterior, incluso en casos donde puede haberse producido una vulneración de derechos, impide que las personas afectadas puedan tener a su disposición recursos efectivos para obtener reparación y compensación por los daños sufridos.

El Tribunal Europeo de Derechos Humanos ha establecido que si bien la seguridad nacional puede considerarse como un fin legítimo para limitar el derecho a la privacidad, el simple hecho de que la persona no conozca que está siendo vigilada no implica que su derecho a la privacidad reconocido en el art. 8 del CEDH pueda ser igualmente vulnerado. En este sentido es inaceptable que la seguridad del disfrute de un derecho garantizado por el Convenio pueda desaparecer por el simple hecho de que la persona no tenga conocimiento de su violación.[19] Igualmente, el tribunal ha mantenido que el poder de realizar una vigilancia secreta de ciudadanos solo puede ser tolerado cuando es estrictamente necesario para salvaguardar las instituciones democráticas. Esto significa en la práctica que debe haber garantías efectivas contra el abuso.[20]

17 Art. art. 588 ter i

18 STS 1094/2010 de 10 de diciembre.

19 *Klass and others v. Germany*, 6 September 1978, para. 36

20 Kennedy v. The United Kingdom, 18 May 2010, para. 153

CONCLUSIÓN

Los sistemas de vigilancia actuales son difíciles de detectar y por lo tanto se prestan a un uso abusivo. No hay ninguna duda de que estos sistemas suponen una grave amenaza para derechos humanos como el derecho a la privacidad y otros derechos como el de libertad de expresión y asociación. Tal y como han recomendado los organismos internacionales de derechos humanos, los servicios de inteligencia deben estar supervisados ya sea por mecanismos internos, parlamentarios o judiciales con capacidad de investigaciones de oficio. Los órganos de supervisión no deben ejercer solo control ex ante, sino también debe existir la posibilidad de un control posterior. Sus decisiones deben poder ser revisadas por organismos independientes e imparciales en cada fase.

Cuando se establezcan tribunales especiales para ejercer estas funciones, deben ser independientes e imparciales, deben celebrar todas las audiencias en público, a menos que existan motivos específicos e imperiosos en un caso concreto, y deben estar facultados para revisar la legalidad de la legislación sobre vigilancia de las comunicaciones, anular las decisiones de vigilancia de las comunicaciones y ordenar soluciones efectivas. Los mecanismos de supervisión parlamentaria deben tener un mandato, una independencia y unas competencias suficientes para garantizar que los organismos gubernamentales, incluidas las fuerzas del orden y los servicios de inteligencia, rindan cuentas realmente de sus actos.

La legislación debe contemplar que toda persona que crea que sus derechos han sido vulnerados tiene mecanismos adecuados para poder reclamar una reparación efectiva, como la plena compensación por los daños sufridos.

En **España** está claro que muchos ciudadanos se enfrentan, indefensos, a violaciones de derechos humanos, que suponen injerencias arbitrarias en su vida privada, su domicilio o su correspondencia en violación de la Constitución y el Convenio Europeo de Derechos Humanos.

La falta de mecanismos de supervisión independiente e imparcial a posteriori dentro la normativa que regula el CNI, así como la propia Ley de Secretos Oficiales, dificultan enormemente que las personas que consideren que han sido objeto de vigilancia de manera arbitraria o ilícita puedan presentar denuncias sobre estas actuaciones. Cuando la normativa no contiene salvaguardas para evitar excesos cometidos bajo el supuesto interés de la seguridad nacional, es difícil que las demandas judiciales tengan éxito.

El Gobierno, además, no ha actuado con transparencia al negarse a revelar información sobre adquisición y uso de herramientas de espionaje tipo Pegasus que pueden llevar a vulneraciones graves de derechos humanos.

Las autoridades españolas han actuado con una doble vara de medir injerencias ilegales a través de Pegasus en España. Mientras presentaban denuncias en la Audiencia nacional relativa al espionaje de la infección de teléfonos oficiales no iniciaban ningún tipo de investigación o denuncia relativa a decenas de teléfonos de ciudadanos infectados por Pegasus, y cuyas terminales no habían sido objeto, en principio, de investigación por parte del CNI.

RECOMENDACIONES:

Con el fin de lograr llegar a la verdad de lo ocurrido, establecer medidas de reparación a las víctimas de violaciones de derechos humanos y evitar que se repitan los episodios de injerencia arbitraria y masiva y vulneración de derechos humanos, AI pide que se pongan en marcha las siguientes medidas:

SOBRE INVESTIGACIÓN DE LO OCURRIDO:

1.- Llevar a cabo una investigación exhaustiva, independiente y eficaz sobre los casos de vigilancia masiva de personalidades catalanas, incluyendo la apertura de una Comisión específica que investigue este supuesto espionaje y cuyos resultados se pongan a disposición de la Comisión ad hoc del Parlamento Europeo sobre las infracciones de la legislación de la UE asociadas al uso de Pegasus.

2.- Promover un compromiso inequívoco entre el Estado y la Fiscalía General del Estado para colaborar con las investigaciones judiciales abiertas y que puedan abrirse, incluyendo la propuesta de pruebas, recogida de evidencias y búsqueda diplomática de colaboración de la empresa NSO y del Estado de Israel con las investigaciones.

PARA IMPEDIR QUE SE REPITA

3.- Garantizar una legislación nacional que imponga salvaguardias contra las violaciones de los derechos humanos mediante la vigilancia digital, en consonancia con los Principios de Necesidad y Proporcionalidad, y que establezca mecanismos de rendición de cuentas, causas de acción, etc., diseñados para proporcionar a las víctimas de abusos de vigilancia una vía de recurso

4.- Aumentar el control y las garantías legales y operativas en las operaciones de vigilancia a través de:

- Una revisión de la legalidad continuada y continua en los procedimientos del CNI, así como un control judicial adecuado, incluyendo también lo relativo al almacenamiento de la información obtenida, con sistemas sólidos e independientes de supervisión, para evitar actuaciones arbitrarias o abusivas.
- Introducir en la normativa española mecanismos efectivos e imparciales de supervisión y control de las actividades de vigilancia. Para ello se debe modificar la normativa que regula el CNI y el control de sus actuaciones para asegurar que su actuación y los mecanismos de control de la misma son acordes con los estándares de derechos humanos.
- Modificar la Ley de Secretos Oficiales para adecuarla a los estándares internacionales sobre clasificación de información reservada y que los posibles abusos y violaciones de los derechos humanos no puedan ampararse bajo la consideración de secreto, y queden por lo tanto impunes.

5.- Proporcionar a las víctimas de violaciones de derechos humanos en el marco de injerencias arbitrarias y masivas en su ámbito familiar y privado, instrumentos efectivos de defensa de sus derechos y de reparación siguiendo la doctrina del TEDH.

SOBRE SISTEMAS DE VIGILANCIA MASIVA Y CONCRETAMENTE EL PROGRAMA PEGASUS Y NSO GROUP:

6.- A nivel nacional, el Gobierno debe suspender el uso, venta y transferencia de estos instrumentos de vigilancia hasta que se instaure un marco regulador adecuado y respetuoso con los derechos humanos.

7.- A nivel internacional, las autoridades españolas deben impulsar y apoyar la imposición de una moratoria sobre el uso, venta y transferencia de estos equipos de vigilancia hasta que se establezca un marco reglamentario adecuado de derechos humanos al respecto.

8.- Las autoridades españolas deben revelar información sobre todos los contratos —pasados, en vigor o futuros— que tengan con empresas privadas de vigilancia, respondiendo a las solicitudes de información o tomando ellos mismos la iniciativa de publicarla.

9.- Aplicar normas de contratación que restrinjan los contratos públicos de tecnología y servicios de vigilancia a aquellas empresas que se adhieran a los Principios Rectores de la ONU y que no hayan prestado servicios a clientes que cometan abusos en materia de vigilancia

10.- Participar en los principales esfuerzos multilaterales (por ejemplo, en apoyo del llamamiento del Relator Especial de la ONU para que se establezca una moratoria inmediata sobre la venta, la transferencia y el uso de la tecnología de vigilancia) para desarrollar normas sólidas de derechos humanos que regulen el desarrollo, la venta y la transferencia de equipos de vigilancia e identificar los objetivos no permitidos de la vigilancia digital.

AMNISTÍA
INTERNACIONAL