SÍNTESIS

Estudio para la Comisión PEGA

Parlamento Europeo

# Las repercusiones de Pegasus para los derechos fundamentales y los procesos democráticos [1]


RESUMEN

En el presente estudio - que ha sido encargado por el Departamento Temático de Derechos de los Ciudadanos y Asuntos Constitucionales del Parlamento Europeo a petición de la Comisión de Investigación Encargada de Examinar el Uso del Programa Espía de Vigilancia Pegasus y Otros Programas Equivalentes (PEGA) - se analizan las repercusiones del uso de Pegasus y programas espía similares para los valores del artículo 2 del TUE, la privacidad y la protección de datos, así como para los procesos democráticos de los Estados miembros.


## Contexto

La vigilancia específica basada en herramientas tecnológicas plantea inquietudes justificadas debido a su profundidad, dado que puede extenderse a todos los aspectos de la vida de las personas a las que va dirigida. Los sistemas de programas espía que piratean dispositivos móviles —como Pegasus, desarrollado por el grupo israelí NSO— permiten llevar a cabo una vigilancia secreta generalizada. Pegasus cuenta con un acceso total y sin restricciones al dispositivo pirateado: es capaz de extraer todos los datos que contiene (extracción inicial de datos), controlar todas las actividades que se realizan a través de él (seguimiento pasivo), activar las funcionalidades del dispositivo para obtener más datos (seguimiento activo) y, posiblemente, interferir en su contenido y en los mensajes que se envían desde él (manipulación). Puede instalarse sin que las personas afectadas realicen ninguna acción y sin dejar rastro alguno de su funcionamiento (o, al menos, un rastro muy escaso).

## Objetivo

El objetivo del presente informe es a) determinar cuáles son las cuestiones esenciales relativas al modo en que Pegasus y otros programas espía pueden interferir en los derechos individuales y los procesos e instituciones democráticos, b) evaluar el marco jurídico pertinente, c) determinar en qué medida y según qué condiciones se pueden utilizar los programas espía de forma lícita, y d) recomendar formas de aplicar tales condiciones.

### Impacto sobre los derechos y la democracia

La vigilancia generalizada afecta a la privacidad de las personas, a la protección de datos y a otros derechos individuales - como los derechos a la libertad de expresión, asociación y reunión—, así como a las instituciones democráticas de la sociedad. Los programas espía condicionan la participación política en el sentido de que los ciudadanos que han sido vigilados pueden sentirse obligados a abstenerse de llevar a cabo interacciones de

[1] Estudio completo en inglés: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU(2022)740514_EN.pdf


Departamento Temático de Derechos de los Ciudadanos y Asuntos Constitucionales
Dirección General de Políticas Interiores
PE 740.514 – Mayo de 2023

SR 1270231ES

carácter político, expresar sus opiniones con sinceridad y asociarse con otras personas con fines políticos. Esto afecta a la calidad de una esfera pública democrática, que en última instancia depende de las aportaciones y reacciones de los ciudadanos. En concreto, los programas espía afectan a individuos (como periodistas, políticos y activistas) que desempeñan un papel especial en la esfera pública. Vigilar a estas personas abre las puertas a la represión, la manipulación, el chantaje, la falsificación y la difamación. Es posible influir hasta en el propio proceso electoral, puesto que la información obtenida, posiblemente manipulada, se emplea para llevar a cabo campañas de desprestigio contra candidatos señalados o para emprender otras acciones que afecten a sus probabilidades de obtener buenos resultados electorales. El mero temor a ser espiado puede llevar a las personas a abstenerse de concurrir para un cargo o de emprender una campaña eficaz.

**Programas espía y seguridad nacional**

El uso de programas espía se suele justificar alegando motivos relacionados con la seguridad nacional o la ejecución de las leyes. No obstante, parece que en muchos casos los programas espía se utilizan con otros fines, a menudo ligados a objetivos políticos partidistas o a la represión de la disidencia social y política. Es sabido que muchos Estados han mencionado la seguridad nacional como un pretexto jurídico cínico para restringir la libertad de expresión, legitimar la tortura y otros malos tratos, y para ejercer un efecto paralizador sobre minorías, activistas y la oposición política. En concreto, existen numerosas pruebas de que Pegasus se ha utilizado para vigilar a personas que no tienen ninguna relación con delitos graves o amenazas para la seguridad nacional, como oponentes políticos, activistas de los derechos humanos, abogados y periodistas. Para evitar un uso expansivo de la noción de seguridad *nacional*, esta debe entenderse de forma restrictiva y diferenciarse del concepto de seguridad *interior*, ya que este último tiene un ámbito de aplicación más amplio que incluye la prevención de riesgos para ciudadanos particulares y, de forma especial, la aplicación del Derecho penal.

**Legislación internacional en materia de derechos humanos**

En el marco de las Naciones Unidas, las actividades de vigilancia deben evaluarse conforme a tratados de derechos humanos como el Pacto Internacional de Derechos Civiles y Políticos. El abuso de la vigilancia afecta no solo al derecho a la privacidad, sino también a la libertad de expresión y a otros derechos recogidos en el Pacto. Tanto la privacidad como la libertad de expresión solo se pueden limitar por medio de la ley y según sea necesario con fines legítimos. La seguridad nacional puede justificar una limitación, pero en el caso de Pegasus, es probable que no se satisfagan los requisitos de legalidad y necesidad.

Según el Convenio Europeo de Derechos Humanos, los requisitos de legitimidad, legalidad, necesidad y proporcionalidad, en el contexto de una sociedad democrática, se aplican en todos los supuestos de vigilancia específica. Una extensa jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH) ha establecido las condiciones para que la vigilancia encubierta sea coherente con los derechos humanos, sobre todo en lo relativo a la legalidad (accesibilidad de las leyes que autorizan la vigilancia y previsibilidad de sus consecuencias) y la notificación. El Tribunal también ha concedido legitimación a personas que incluso solo hayan sido potencialmente afectadas por una vigilancia encubierta.

**Derecho de la Unión**

En el contexto del Derecho de la Unión, la vigilancia específica es pertinente para los derechos que se incluyen en la Carta de los Derechos Fundamentales de la Unión Europea, para los principios contenidos en los Tratados (como la democracia y el Estado de Derecho) y para diversos instrumentos del Derecho derivado de la Unión, como los que se refieren a la protección de datos.

Según el Tratado de la Unión Europea (TUE), la seguridad nacional es responsabilidad exclusiva de cada uno de los Estados miembros, pero, en principio, esto no excluye que las actividades relacionadas con la seguridad nacional estén sujetas al Derecho de la Unión, algo que sí ocurre cuando interfieren en actividades que se encuentran reguladas por el Derecho de la Unión.

No obstante, la aplicación del Derecho de la Unión al uso de programas espía con fines de seguridad nacional encuentra un obstáculo en el hecho de que la seguridad nacional queda excluida del ámbito de aplicación de dos instrumentos fundamentales: el RGPD y la Directiva sobre la privacidad y las comunicaciones electrónicas. Esto puede justificarse a duras penas atendiendo a los derechos consagrados en la Carta y los principios que se recogen en los Tratados. Debido a que esta exclusión puede utilizarse de forma demasiado amplia, cabe señalar

que solo se refiere a aquellos casos en que los programas espía se utilizan realmente para proteger la seguridad nacional bien entendida. El Derecho de la Unión se aplica íntegramente al uso de investigaciones encubiertas con fines de ejecución de las leyes. Sin embargo, incluso en este ámbito, existen pruebas de que se han cometido abusos.

**Recomendaciones**

El uso de programas espía representa una amenaza para los derechos fundamentales y los principios básicos del Derecho de la Unión, como la democracia (representativa-deliberativa) y el Estado de Derecho. Existe el riesgo de que se debiliten los principios mismos en los que se asienta el ordenamiento jurídico de la Unión.

En los ordenamientos jurídicos internacional y europeo, las actividades relacionadas con la seguridad nacional pueden justificar restricciones de los derechos fundamentales, pero para que estas sean lícitas tienen que cumplir las condiciones de *legitimidad*, *legalidad*, *necesidad*, *equilibrio* y *coherencia con la democracia*.

En muchas de las ocasiones en que se ha desplegado, Pegasus ha incumplido hasta ahora estos requisitos porque se ha utilizado con fines ilegítimos, sin un marco jurídico adecuado, en ausencia de una necesidad real, provocando un daño desproporcionado a los derechos individuales y socavando la democracia.

Se proponen varias estrategias que pueden ayudar a prevenir los abusos:

- Circunscribir el ámbito material de las actividades relacionadas con la seguridad nacional para que a los Estados les resulte más difícil utilizar la seguridad nacional como justificación jurídica espuria para llevar a cabo actividades encaminadas a otros fines.
- Circunscribir el ámbito de aplicación personal de las actividades relacionadas con la seguridad nacional, excluyendo de este determinadas actividades que realizan partes particulares.
- Incluir la actividad relacionada con la seguridad nacional en el ámbito de aplicación de la legislación en materia de protección de datos para garantizar que las restricciones de los derechos de los titulares de los datos con fines de seguridad nacional estén sujetas a requisitos de legalidad y proporcionalidad.
- Apoyar la adopción de marcos jurídicos adecuados en el contexto nacional, puesto que la seguridad nacional sigue siendo una competencia reservada a los Estados miembros y es a ellos a quienes corresponde garantizar eficazmente que su actividad se ajuste a los derechos fundamentales y los principios del Derecho de la Unión. Estos marcos deben cumplir principios como los siguientes: legalidad, fin legítimo, necesidad, proporcionalidad, autoridad competente, tutela judicial efectiva, notificación al usuario, transparencia, supervisión pública, seguridad y certificación, y adecuación técnica.

Una moratoria políticamente viable sobre el uso de herramientas de pirateo de dispositivos podría consistir en una presunción firme contra la licitud de su uso, presunción basada en pruebas exhaustivas de que se ha abusado de su utilización. Esta presunción solo podría superarse cuando un Estado demostrase de forma convincente su voluntad y capacidad para evitar todo tipo de abusos.

Además, se debe instar a todos los Estados miembros a que prohíban el uso de herramientas de programas espía específicas cuando, como ocurre con Pegasus, existan pruebas sólidas de que se han utilizado ampliamente en actividades ilícitas, sobre todo dentro de la Unión. Hasta que no haya pruebas claras de que ya no se llevan a cabo esas prácticas inaceptables, seguir desplegando Pegasus, incluso en el marco de actividades lícitas, supone apoyar a sus creadores y desarrolladores y, por tanto, implica una complicidad política (si bien no jurídica) con tales prácticas.

Autores externos:
Prof. Dr. Giovanni SARTOR, Universidad de Bolonia e Instituto Universitario Europeo
Prof. Dr. Andrea LOREGGIA, Universidad de Brescia

Administrador responsable de la investigación: Mariusz MACIEJEWSKI Asistente de edición: Ivona KLECAN
Contacto: poldep-citizens@europarl.europa.eu

Este documento está disponible en la siguiente dirección de internet: www.europarl.europa.eu/supporting-analyses.

PE 740.514
IP/C/PEGA/IC/2022-071

Versión impresa ISBN 978-92-848-0547-1 | doi: 10.2861/026923 | QA-04-23-457-ES-C
Edición en PDF ISBN 978-92-848-0539-6 | doi: 10.2861/824166 | QA-04-23-457-ES-N