Pegasus: análisis de su impacto en los derechos fundamentales en Europa

Mathilde Raebisch
College of Europe
mathilde.raeb@gmail.com
ORCID: 0009-0001-4116-682X

Recepción: 09/11/2023
Aceptación: 18/01/2024
Publicación: 31/01/2024

Cita recomendada: RAEBISCH, M. (2024). "Pegasus: análisis de su impacto en los derechos fundamentales de las personas en Europa". *Quaderns IEE: Revista de l'Institut d'Estudis Europeus*, *3*(1), 62-87.
DOI: <https://doi.org/10.5565/rev/quadernsiee.66>

Resumen

En 2021, se destapó el uso del programa espía Pegasus por varios Estados del mundo, incluyendo numerosos Estados europeos, tanto miembros de la Unión Europea como parte en el Consejo de Europa. Las distintas investigaciones que se llevaron a cabo por parte de periodistas y otras personas de la sociedad civil, así como por parte de las propias instituciones europeas, permiten entender que el uso de este programa constituye una grave injerencia en varios derechos humanos. Sin embargo, dicho uso puede verse justificado, siempre que se respeten una serie de requisitos normativos, así como jurisprudenciales elaborados a nivel de la Unión Europea y del Consejo de Europa.

Palabras clave: Injerencia; Uso abusivo; Privacidad; Unión Europea; Consejo de Europa.

Abstract. *Pegasus: analysis of its impact on fundamental rights in Europe*

In 2021, the use of the spying program Pegasus by several States worldwide was uncovered, including numerous European States, both European Union member States and contracting States to the Council of Europe. The various investigations that were carried out, by journalists and other civil society actors as well as by European institutions themselves, enable the reader to understand that the use of such program

constitutes a serious interference with a number of human rights. Nevertheless, the use of this program could be justified, both at European Union and Council of Europe level, provided it complies with a series of normative and jurisprudential requirements.

Keywords: Interference; Abusive use; Privacy; European Union; Council of Europe.

Resum. *Pegasus: anàlisi del seu impacte en els drets fonamentals a Europa*

El 2021, es va destapar l'ús del programa espia Pegasus per diversos Estats del món, incloent nombrosos Estats europeus, tant membres de la Unió Europea com a part al Consell d'Europa. Les diferents investigacions que es van dur a terme per part de periodistes i altres persones de la societat civil, així com per part de les institucions europees mateixes, permeten entendre que l'ús d'aquest programa constitueix una greu ingerència en diversos drets humans. Això no obstant, aquest ús es pot veure justificat, sempre que es respectin una sèrie de requisits normatius, així com jurisprudencials elaborats a nivell de la Unió Europea i del Consell d'Europa.

Paraules clau: Ingerència; Ús abusiu; Privacitat; Unió Europea; Consell d'Europa.

Sumario

1. INTRODUCCIÓN

El 11 de septiembre de 2001, se produjeron, en Estados Unidos, los atentados más mortíferos de la historia occidental, pues 2977 personas perecieron y otras 6291 resultaron heridas. Dichos atentados constituyeron el punto de inflexión con respecto al poder de vigilancia e investigación de todos los Estados del mundo. Más recientemente, en la década de 2010, Europa fue el teatro de varios atentados, como, por ejemplo, los atentados del 13 de noviembre de 2015, en París; del 22 de marzo de 2016, en Bruselas; del 14 de julio de 2016; en Niza; y del 11 de diciembre de 2018, en Estrasburgo. Este flagrante incremento del terrorismo ha dado lugar a la adopción de leyes cada vez más invasivas y que permiten, en base a motivos de seguridad, acceder a las comunicaciones de los individuos de manera cada vez más amplia. Así, en Francia, tras los atentados del 13 de noviembre de 2015, se modificó el artículo L 851-2-I del llamado *Code de la Sécurité intérieure*, permitiendo, para prevenir el terrorismo, que se recabara información sobre los datos de conexión, no sólo de una persona que se identifique como una amenaza, sino también de las personas de su entorno, siempre que estas sean susceptibles de proporcionar información para los fines para los que se concedió la primera autorización.

Fue en este contexto que se destaparon los abusos cometidos por los gobiernos de varios Estados del mundo, mediante el uso del llamado programa espía (en inglés, *spyware*) Pegasus. Este tipo de programas son programas maliciosos que monitorizan la actividad de los dispositivos infectados y que recaban toda la información, personal o no, que pueden contener. Así, la primera investigación periodística que se realizó, en el año 2021, puso de relieve que más de cincuenta mil números de teléfono habían sido infectados por Pegasus. Dichos teléfonos pertenecían, sobre todo, a hombres políticos, periodistas, y defensores de los derechos humanos. El importante revuelo generado por este descubrimiento ha puesto de relieve el grave impacto que tales programas pueden tener en los derechos fundamentales, que se amparan tanto en tratados internacionales como en disposiciones del Consejo de Europa, de la Unión Europea (UE, en adelante) e internas.

Puesto que dicha injerencia puede causar daños importantes a los derechos y libertades de los individuos, e incluso a la democracia y al Estado de Derecho, los

Estados europeos, para legitimar su uso, deben respetar las exigencias establecidas por la UE y/o por el Consejo de Europa. En caso de no respetarlas, estarán vulnerando los derechos de las personas espiadas, las cuales deberán tener la posibilidad de denunciar dicha situación. Subrayar que, si bien el Consejo de Europa y la UE son dos organizaciones regionales europeas, no tienen la misma estructura normativa y judicial y, por lo tanto, dichas exigencias pueden variar.

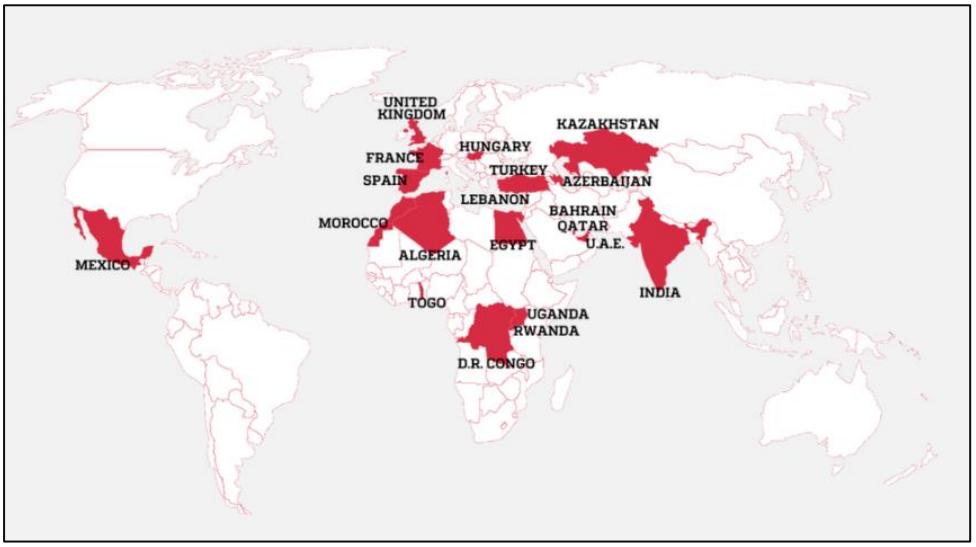
Partiendo de lo anterior, en el presente trabajo, se persigue revelar cómo Pegasus ha tenido un impacto en los derechos fundamentales en Europa. De ahí que éste se divida en dos títulos. El primero tratará específicamente de Pegasus y determinará cómo funciona dicho programa y cómo se ha utilizado (y seguramente se sigue utilizando) por los Estados de la UE. Efectivamente, si bien se acusa a España de haber hecho uso del mismo, se sospecha que otros Estados de la Unión también lo han usado (véanse, por ejemplo, Polonia, Hungría, Grecia y Chipre). El segundo título se detendrá en el análisis de los distintos derechos posiblemente vulnerados por Pegasus (el derecho a la vida privada y familiar, el derecho al respeto de los datos de carácter personal, el derecho a la tutela judicial efectiva, etc.). Aunque su uso constituya una injerencia en dichos derechos, esa injerencia se podrá justificar siempre que se respeten una serie de requisitos normativos, así como jurisprudenciales.

2. PEGASUS COMO HERRAMIENTA DE VIGILANCIA SECRETA: SU FUNCIONAMIENTO Y USO POR LOS ESTADOS DE LA UNIÓN EUROPEA

Se destapó el uso de Pegasus por los gobiernos de varios Estados del mundo, gracias a la investigación periodística publicada el 18 de julio de 2021, por *Forbidden Stories*, con ayuda de *Amnesty International*.[1] Aparte de denunciar la infección, desde 2016, de más de cincuenta mil números de teléfono, *Forbidden Stories* también reveló que al menos ciento ochenta periodistas fueron seleccionados como objetivos del programa Pegasus, especialmente en India, México, Marruecos y Francia.[2]

Este programa también se ha utilizado para espiar a "defensores de los derechos humanos, miembros de partidos políticos de la oposición, empresarios e incluso jefes de Estado" (Rueckert, 2021).

[1] Amnesty International: 'Comunicado de prensa: Una filtración de datos masiva revela que el software espía de la empresa israelí NSO Group se utiliza para atacar a activistas, periodistas y figuras políticas en todo el mundo', 19 de julio de 2021..
[2] *Ibidem*.



Mapa 1. Países en los que viven los periodistas víctimas del programa Pegasus. (Fuente: Forbidden Stories)

2.1. Presentación del programa Pegasus

Este programa que fue creado y comercializado en 2013, por la empresa israelí *NSO Group* (Bouchenni y Gay-Padona, 2022) (la cual fue creada en 2010) y permite al autor del ataque leer los mensajes del usuario y el correo, escuchar las llamadas, realizar capturas de pantalla, registrar las teclas pulsadas, acceder al historial del navegador, a los contactos, recibir video en directo de aplicaciones como *Facetime* y *Skype*, tener acceso a correos electrónicos —incluso con sus datos adjuntos—, activar cámaras y micrófonos y vaciar toda la información contenida en el dispositivo (Hernández, et al., 2019).

También se tendrá acceso a los datos que se introduzcan en el teclado del dispositivo, y a todas las comunicaciones escritas mantenidas con otros dispositivos. Incluso, serán visibles las contraseñas guardadas en el mismo[3].

Si bien *NSO Group* (2021) afirma que el programa Pegasus no es "una tecnología de vigilancia masiva y solo recopila datos de los dispositivos móviles de personas concretas sospechosas de estar implicadas en delitos graves y actos terroristas", en realidad ha sido usado para fines totalmente distintos, pues los Estados lo han utilizado para espiar a personas que no eran ni terroristas ni delincuentes.[4]

Así, por ejemplo, *Front Line Defenders* y *Citizen Lab* revelaron que los teléfonos de cuatro defensores de los derechos humanos jordanos habían sido infectados por Pegasus entre 2019 y 2021 (Al-Maskati, 2022). *Forbidden Stories* también hizo hincapié en el posible uso de Pegasus para llevar a cabo el asesinato de Jamal Khashoggi,

[3] Consejo de Europa: 'Report: Pegasus spyware and its impacts on human rights', *cit.,* pág. 8.
[4] Alto Comisionado de las Naciones Unidas para los Derechos Humanos: 'The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights', 4 de agosto de 2022.

periodista y oponente político saudí (Álvarez, 2022). Incluso el Relator Especial de las Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y expresión remarca que la vigilancia secreta conduce "a detenciones arbitrarias, a veces a torturas y, posiblemente, a ejecuciones extrajudiciales".[5]

Aunque se puede imaginar que Pegasus sólo se ha utilizado en países totalitarios (u otros regímenes políticos poco democráticos), también se ha usado en Estados de la UE, aun cuando el propio Tratado de la Unión Europea (TUE, en adelante)[6] establece que la Unión se fundamenta en los valores de respeto de la dignidad humana, libertad, democracia, igualdad, Estado de Derecho y respeto de los derechos humanos[7] y que los Estados, para ingresar como miembros, deberán respetar estos valores.[8]

2.2. El uso de Pegasus por los Estados miembros de la Unión Europea

Según la Comisión del Parlamento Europeo encargada de examinar el Uso del Programa Espía de Vigilancia Pegasus y Otros Programas Equivalentes[9] (Comisión PEGA, en adelante), al menos cuatro Estados miembros de la UE han hecho un uso ilegítimo de Pegasus (Polonia, Hungría, Grecia y España[10]). Dicha Comisión también menciona el importante papel que desempeñó Chipre al exportar Pegasus hacia otros países.

2.2.1. España y el *CatalanGate*

Con relación a España, dicho caso se conoce como el *CatalanGate* y, según el laboratorio de investigación *Citizen Lab*, a partir de 2017, y posiblemente ya en 2015, los teléfonos de los ciudadanos catalanes fueron objeto de una operación a gran escala en la que se utilizó un software espía de la empresa mercenaria de vigilancia *NSO Group*.[11]

De ahí que *Citizen Lab* identificó a sesenta y cinco personas relacionadas con el independentismo catalán que fueron objeto de espionaje (Scott-Railton, et al., 2022) y al menos sesenta y tres de ellas mediante Pegasus[12].

---

[5] Relator Especial de las Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y expresión: 'Surveillance and human rights: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expresión', A/HRC/41/35.
[6] *OJ C 326, 26.10.2012, págs. 13 a 390.*
[7] Véase el artículo 2 TUE.
[8] Véase el artículo 49 TUE.
[9] A estos efectos, véase Decisión del Parlamento Europeo, de 10 de marzo de 2022, sobre la constitución, el objeto de la investigación, las competencias, la composición numérica y la duración del mandato de la Comisión de Investigación encargada de examinar el uso del programa espía de vigilancia Pegasus y otros programas equivalentes (2022/2586(RSO)), Considerando A.
[10] Comisión PEGA: 'Draft report', 8 de noviembre de 2022, pág. 5.
[11] The Citizen Lab: '¿Harías Clic? – Una historia de The Citizen Lab', 23 de diciembre de 2022.
[12] *Ibidem*.

Case type	Number observed
Individuals with forensically confirmed infections	51
Individuals targeted via SMS or WhatsApp with Pegasus infection attempts, without forensic confirmation of a successful infection	12
Total Pegasus targets	63

Tabla 1. Panorama general de las personas infectadas por el programa Pegasus (Fuente: Citizen Lab)[13]

Por ejemplo, cuatro miembros catalanes del Parlamento Europeo que apoyaron la independencia fueron afectados por Pegasus, bien de manera directa (Diana Riba y Jordi Solé), o bien de manera indirecta (Clara Ponsati y Carles Puigdemont).[14]

También fueron objeto de espionaje, varios miembros de *Òmnium Cultural* y de la Asamblea Nacional Catalana, dos organizaciones de la sociedad civil catalana a favor del movimiento independentista.[15] De la misma manera, fueron espiadas personalidades como Joan Matamala, que trabajan para el desarrollo del *software* libre y del voto digital.[16]

Igualmente, varios abogados, como Gonzalo Boye y Jaume Alonso-Cuevillas (abogados de Carles Puigdemont); así como Andreu Van den Eynde (abogado de Oriol Junqueras, Roger Torrent, Raül Romeva y Ernest Maragall) fueron infectados.[17]

Finalmente, *Citizen Lab* subraya que mediante Pegasus también se infectaron los dispositivos de varios políticos catalanes.

Presidentes de *la Generalitat de Catalunya* infectados por el programa Pegasus	**Momento en que fueron espiados**
Pere Aragonès (actual presidente de la *Generalitat*)	Cuando era vicepresidente
Joaquim Torra (expresidente de la *Generalitat*)	Durante su mandato
Carles Puigdemont (expresidente de la *Generalitat*)	De manera indirecta
Artur Mas (expresidente de la *Generalitat*)	Terminado su mandato

Tabla 2. Presidentes de la Generalitat de Catalunya afectados por el uso del programa Pegasus (Fuente: Elaboración propia con base en los datos proporcionados por Citizen Lab)[18]

Presidentes del *Parlament de Catalunya* infectados por el programa Pegasus	**Momento en que fueron espiados**
Laura Borràs (expresidenta del *Parlament*)	Cuando era miembro del Congreso de Diputados.
Roger Torrent (expresidente del *Parlament*)	Durante su mandato

Tabla 3. Presidentes del Parlament de Catalunya afectados por el uso del programa Pegasus (Fuente: Elaboración propia con base en los datos proporcionados por Citizen Lab)[19]

[13] *Ibidem*, pág. 6.
[14] *Ibidem*, pág. 8.
[15] *Ibidem*.
[16] *Ibidem*, pág. 10
[17] *Ibidem*.
[18] *Ibidem*, págs. 10 y 11.
[19] *Ibidem*, pág. 11.

Según *Citizen Lab*, existen indicadores que permiten asumir que esa vigilancia fue llevada a cabo por las autoridades españolas.[20] En este sentido, el 5 de mayo de 2022, la exdirectora del Centro Nacional de Inteligencia admitió, ante la Comisión de Secretos Oficiales del Congreso de los Diputados, que los servicios de inteligencia habían investigado, después de haber recabado la correspondiente autorización judicial, a dieciocho independentistas catalanes (Tomás y Orovio, 2022). Respecto de las 47 personas restantes, todavía se desconoce si se ha obtenido o no dicha autorización.

2.3. La situación en otros Estados miembros

Si bien la Comisión PEGA estudia la situación en otros Estados de la Unión, se refiere en especial a España (véase *supra*), Polonia, Hungría, Grecia y Chipre. Por lo tanto, este análisis se centrará únicamente en dichos países (Marzocchi & Mazzini, 2022).

En relación con Polonia, *Citizen Lab* ya había denunciado en 2018 el uso de Pegasus, afirmando que personalidades como Krzysztof Brejza, líder del partido de la oposición y Roman Giertych, abogado de Donald Tusk, habían sido espiados.

Respecto a Hungría, más de 300 personas habrían sido víctimas de Pegasus, por ejemplo, Brigitta Csikász investigaba la malversación de fondos europeos por parte de Hungría cuando fue espiada (Verseck, 2022).

En lo que se refiere a Grecia, se ha permitido la exportación de Pegasus y programas espía a Estados con estándares de derechos humanos muy débiles.[21] Igualmente, varias personalidades griegas han sido objeto de espionaje. Por ejemplo, Nikos Androulakis, líder de un partido político de la oposición y miembro del Parlamento Europeo fue espiado mediante *Predator* (programa espía equivalente a Pegasus). En total, 33 personalidades griegas fueron presuntamente espiadas por dicho programa (Stamouli, 2022).

Chipre, por su parte, constituye un núcleo de exportación[22] y es un lugar atractivo para el comercio de tales programas, pues sus leyes se aplican de manera laxa.[23]

Es importante resaltar que Pegasus ha sido utilizado de manera abusiva por varios Estados miembros de la UE. El problema que entraña este uso abusivo es que Pegasus (como los demás programas espía), constituye una injerencia en los derechos fundamentales de las personas, lo que puede generar consecuencias muy graves para estas. Sin embargo, y como se analiza *infra*, dicha injerencia puede justificarse.

[20] *Ibidem*, pág. 1.
[21] *Ibidem*. párr. 75 g), pág. 83.
[22] Comisión PEGA: 'REPORT of the Investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware', *cit*., párr. 99, pág. 102.
[23] *Ibidem*.

3. PEGASUS COMO HERRAMIENTA DE VIGILANCIA SECRETA: UNA INJERENCIA EN LOS DERECHOS FUNDAMENTALES Y SU POSIBLE JUSTIFICACIÓN

Como bien subraya Tomás Mallén (2015), la comunidad internacional, incluyendo el Consejo de Europa y la UE, siempre ha tenido la preocupación de conciliar la libertad personal de los individuos con la seguridad. Y para ello, el Estado debe invadir la privacidad de los ciudadanos (Chmielarz, 2022). Efectivamente, "las fuertes políticas de seguridad distorsionan el equilibrio entre la libertad y el derecho a la privacidad y la seguridad del Estado" (Chmielarz, 2022). Esto ilustra que el uso de Pegasus se podrá justificar, aunque constituya una injerencia en los derechos fundamentales. Pero para ello se deberán respetar determinados requisitos.

3.1. Una multitud de derechos posiblemente vulnerados

3.1.1. El derecho a la vida privada y familiar

El derecho a la vida privada constituye el "núcleo esencial" de los derechos de la personalidad (Rebollo, 2008 y Encabo, 2012). De ahí que, entre todos los derechos fundamentales que se pueden vulnerar con el uso de Pegasus, la Comisión PEGA menciona primero este derecho,[24] el cual se encuentra en el artículo 7 de la Carta de Derechos Fundamentales de la UE (CDFUE, en adelante).[25]

En este sentido, el Tribunal de Justicia de la UE (TJUE, en adelante) establece que, para demostrar la existencia de una injerencia en el derecho fundamental al respeto de la vida privada, carece de relevancia que la información relativa a la vida privada de que se trate tenga o no carácter sensible o que los interesados hayan sufrido o no inconvenientes, en razón de tal injerencia.[26]

Para el Consejo de Europa, el simple hecho de que Pegasus permita la vigilancia selectiva, así como la vigilancia indiscriminada, constituye también una injerencia en este derecho,[27] el cual se recoge en el artículo 8, apartado 1 del Convenio Europeo de Derechos Humanos (CEDH, en adelante).[28]

A estos efectos, el Tribunal Europeo de Derechos Humanos (TEDH, en adelante) considera que la mera existencia de una legislación que autoriza un sistema para la vigilancia secreta de las telecomunicaciones implica una amenaza de control para todos aquellos susceptibles de que se les aplique la legislación. Esta amenaza lesiona necesariamente la libertad de comunicación entre los usuarios de los servicios de

[24] Comisión PEGA: 'Draft report', *cit*., párr. 427, pág. 111.
[25] Carta de los Derechos Fundamentales de la Unión Europea, (2016/C 202/02). Según el artículo 7 de la CDFUE, '*Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones*'.
[26] STJUE, Digital Rights Ireland Ltd (asuntos acumulados C-239/12 y C-549/12), 8 de abril de 2014, ECLI:EU:C:2014:238, párr. 33.
[27] Consejo de Europa: 'Pegasus spyware and its impacts on human rights', *cit*., pág. 10.
[28] Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, Roma, 4 de noviembre de 1950.

telecomunicaciones y constituye así una injerencia en el ejercicio de los derechos de los demandantes en virtud del artículo 8, independientemente de las medidas que de hecho se adoptan contra ellos.[29]

3.1.2. El derecho a la protección de datos de carácter personal

El derecho a la protección de datos de carácter personal se encuentra recogido tanto en el derecho primario como en el derecho secundario de la UE. Así, el artículo 8 de la CDFUE reconoce la existencia de dicho derecho, pero omite definir una noción clave: la de dato personal. Y es el Reglamento General de Protección de Datos[30] que aclara qué son datos de carácter personal (Santos, 2020).

En relación con el Consejo de Europa, si bien el CEDH no reconoce este derecho, el Convenio nº 108[31] fue el primer instrumento internacional jurídicamente vinculante en este ámbito y establece "el marco genérico de protección de la persona frente a las posibles intromisiones en sus datos de carácter personal" (Rebollo, 2008). Esto significa que el Convenio nº 108 vela por ampliar la protección de la privacidad, con el objetivo de hacer frente al incremento del tratamiento transfronterizo y automatizado de los datos de carácter personal (Rallo, 2017). Así, el Capítulo II de dicho Convenio recoge los principios básicos para la protección de datos y, a menos que existan garantías apropiadas en el derecho interno, se prohíbe el tratamiento automatizado de los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, los datos de carácter personal relativos a la salud o a la vida sexual, así como los datos de carácter personal que se refieran a condenas penales.[32]

3.1.3. El derecho a la tutela judicial efectiva

El derecho a la tutela judicial efectiva, que constituye uno de los pilares fundamentales del Estado de Derecho, también puede ser objeto de injerencia cuando se utilizan programas espía tipo Pegasus (Milione, 2015).

[29] STEDH, Liberty and others v. The United Kingdom no. 58243/00, 1 de julio de 2008, párr. 56.
[30] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE), OJ L 119, 4.5.2016, p. 1–88.
[31] Convenio de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981 (STE nº 108). Además, hay que estar atentos a cuándo entrará en vigor el Convenio nº 108 + (STCE n.º 223), que es la versión modernizada de este primero.
[32] Véase artículo 6 del Convenio nº 108.

En este sentido, tanto la Comisión PEGA[33] como las Naciones Unidas[34] reconocen que el uso de Pegasus puede conllevar la vulneración de dicho derecho porque permite manipular el dispositivo infectado y falsificar pruebas.[35]

3.1.4. Otros derechos conexos

Tal y como lo indican la Comisión PEGA,[36] el Consejo de Europa[37] y el Alto Comisionado de las Naciones Unidas para los Derechos Humanos,[38] el uso de programas espía también puede suponer la vulneración de otros derechos fundamentales. Así, pueden verse vulnerados el derecho a la libertad de expresión, el derecho de propiedad, la igualdad ante la ley, la no discriminación, la dignidad humana, la libertad de reunión y asociación, la libertad de religión, la integridad física y psíquica de toda persona, etc.

3.2. La posible justificación de tal injerencia

Tal y como explica Chmielarz (2022), por razones de seguridad y para proteger al Estado contra las amenazas a su existencia soberana o a su integridad territorial, las autoridades del Estado pueden justificar la injerencia en los derechos y libertades de las personas considerando la proporcionalidad del método de vigilancia utilizado.

En este sentido, cabe señalar que la seguridad constituye "una condición o un estado que es propio del individuo que vive libre de preocupación o de cualquier afectación de índole mental o física" (Milione, 2020). Para garantizarla, las personas deben ceder parte de su libertad, así como sujetarse a un conjunto de reglas, prescripciones y restricciones (González-Ares, 2021).

Si bien existen varias acepciones de la seguridad (Milione, 2020), se analizará ahora la noción de seguridad nacional,[39] la cual permite a los Estados justificar, hasta

[33] Comisión PEGA: 'Draft report', *cit.*, párr. 427, pág. 111. En el ámbito de la UE, el derecho a la tutela judicial efectiva se encuentra recogido en el artículo 47 CDFUE. En relación con el derecho del Consejo de Europa, la Comisión PEGA afirma que el uso de Pegasus interfiere en el derecho a un proceso equitativo del artículo 6 CEDH. También se puede afirmar que el uso del programa Pegasus puede vulnerar el derecho a un recurso efectivo del artículo 13 CEDH.

[34] Alto Comisionado de las Naciones Unidas para los Derechos Humanos: 'The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights', *cit.*, párr. 11, pág. 4.

[35] *Ibidem*.

[36] Comisión PEGA: 'Draft report', *cit.*, párr. 427, pág. 111, así como párr. 441, pág. 115.

[37] Consejo de Europa: 'Report: Pegasus spyware and its impacts on human rights', *cit.*, págs. 15 a 18 y 19 a 20.

[38] Alto Comisionado de las Naciones Unidas para los Derechos Humanos: 'The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights', *cit.*, párrs. 9 y 10, pág. 4.

[39] Según el informe del Tribunal Europeo de Derechos Humanos: 'Sécurité nationale et jurisprudence européenne' (2013), se incluyen dentro de la noción de seguridad nacional 'la defensa de la seguridad del Estado y del orden constitucional democrático – contra el espionaje, el terrorismo, la apología del terrorismo, el separatismo y la incitación al incumplimiento de la disciplina militar'.

un cierto grado, la injerencia en los derechos de los individuos. Así, en Europa, tanto la UE como el Consejo de Europa prevén los supuestos en que se puede reconocer esa injerencia.

3.2.1. En el ámbito de la Unión Europea

3.2.1.1. La normativa aplicable

Los derechos al respeto de la vida privada y a la protección de los datos de carácter personal, consagrados en los artículos 7 y 8 de la CDFUE, son los principales derechos que se pueden ver afectados por Pegasus. Sin embargo, dichos derechos no son absolutos y, por lo tanto, los Estados miembros pueden justificar que se limiten.[40] A estos efectos, el Supervisor Europeo de Protección de Datos (SEPD, en adelante)[41] remarca que tal limitación siempre debe respetar los criterios previstos en el artículo 52, apartado 1, de la CDFUE. Es decir que debe (a) estar prevista por ley, (b) respetar el contenido esencial de dichos derechos y libertades, (c) responder efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de proteger los derechos y libertades de los demás, (d) ser necesaria, y (e) ser proporcional. Por lo tanto, cualquier medida que implique el tratamiento de datos de carácter personal y/o la vulneración de la vida privada se debe someter a una evaluación de la legalidad, siguiendo los criterios establecidos *supra*.

Así, para determinar si se puede justificar o no el uso de Pegasus, primero se debe analizar si esa limitación en los derechos está prevista por una ley[42] y si dicha ley es accesible y previsible,[43] es decir, si responde a una exigencia de calidad. En caso de no cumplirse dicho requisito, la limitación se considerará ilegal y este control de la legalidad se detendrá.

Sin embargo, si se ha superado la primera parte de la evaluación, se examinará si la medida impugnada respeta el contenido esencial de los derechos afectados.[44] A continuación, se evaluará si esta responde a un objetivo de interés general reconocido

[40] A estos efectos, véase STJUE, Privacy International (asunto C-623/17), 6 de octubre de 2020, ECLI:EU:C:2020:790, párrs. 63 y 64.

[41] SEPD: 'Directrices del SEPD para la evaluación de la proporcionalidad de las medidas que limitan los derechos fundamentales a la intimidad y a la protección de los datos personales', 19 de diciembre de 2019.

[42] En relación con la noción de 'prevista por ley', el Abogado General SAUGMANDSGAARD ØE, H. considera 'necesario (…) que se atribuya a la expresión "prevista por la ley" utilizada en el artículo 52, apartado 1, de la Carta un alcance similar al que dicha expresión tiene en el contexto del CEDH'. STJUE, Tele2 Sverige AB (asuntos acumulados C-203/15 y C-698/15), conclusiones del Abogado General, 19 de julio de 2016, ECLI:EU:C:2016:572, párr. 140. Véase *infra* la jurisprudencia pertinente del TEDH.

[43] SEPD: 'Directrices del SEPD para la evaluación de la proporcionalidad de las medidas que limitan los derechos fundamentales a la intimidad y a la protección de los datos personales', *cit*., pág. 8, nota al pie 11. El SEPD, para entender la noción de 'ley previsible', reenvía a la jurisprudencia del TEDH, citando la sentencia Zakharov v. Russia no. 47143/06, párr. 229

[44] Aquí, el TJUE debe realizar un análisis casuístico, y sus conclusiones al respecto diferirán de un caso a otro.

por la Unión[45] o a la necesidad de proteger los derechos y libertades de los demás. Después, se realizará una evaluación de la necesidad.[46] Finalmente, se realizará una prueba de proporcionalidad.[47]

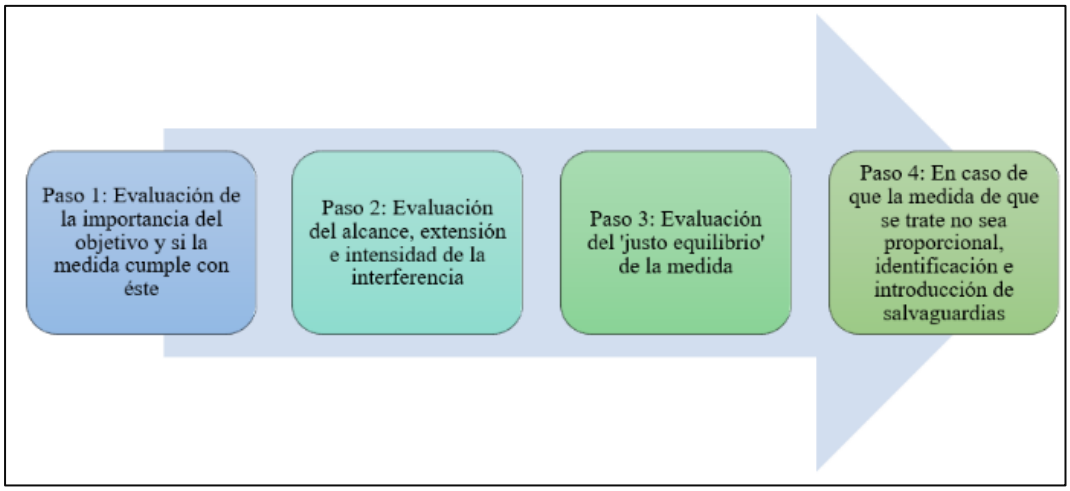


Figura 1. Pasos recomendados por el SEPD para realizar la evaluación de la necesidad (Fuente: Reproducción de la figura del SEPD)

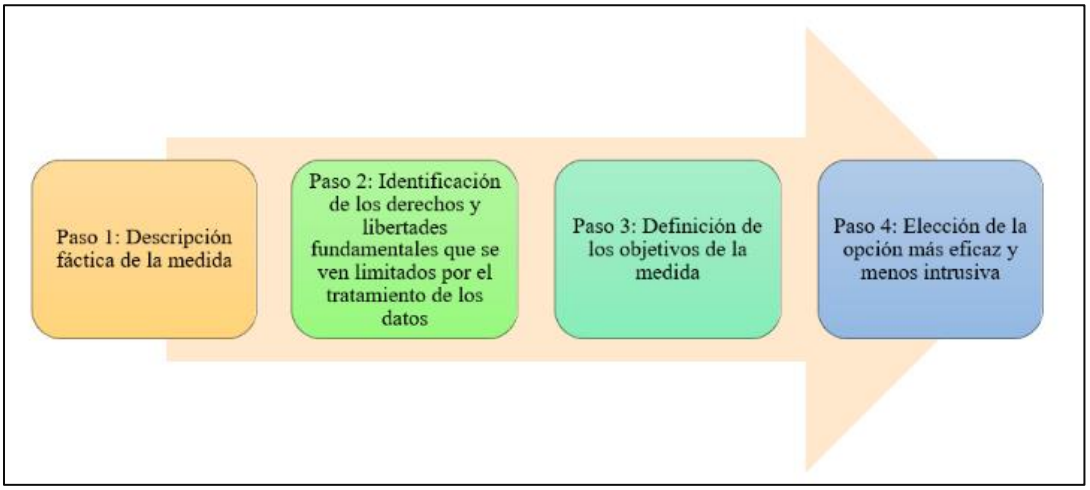


Figura 2. Pasos recomendados por el SEPD para realizar la evaluación de la proporcionalidad (Fuente: Reproducción de la figura del SEPD)

El derecho secundario (o derivado) también recoge los supuestos en que se puede justificar una injerencia en estos derechos. Así, las Directivas 2002/58/CE[48] y

[45] Véase STJUE, Digital Rights, *cit.*, párr. 42: 'De la jurisprudencia del Tribunal de Justicia se desprende que la lucha contra el terrorismo internacional para el mantenimiento de la paz y la seguridad internacionales es un objetivo de interés general de la Unión (…) Lo mismo ocurre en lo que respecta a la lucha contra la delincuencia grave para garantizar la seguridad pública'.
[46] SEPD: 'Manual para la evaluación de la necesidad de las medidas que limiten el derecho fundamental a la protección de datos de carácter personal', 11 de abril de 2017, pág. 5.
[47] STJUE, Digital Rights Ireland Ltd, *cit.*, párr. 46.
[48] Artículo 15, apartado 1, de la Directiva 2002/58/CE.

(UE) 2016/680,[49] así como el Reglamento (UE) 2016/679,[50] recogen los motivos que los Estados miembros pueden utilizar para justificar esa injerencia.

3.2.1.2. La jurisprudencia pertinente

El TJUE se ha pronunciado en varias ocasiones sobre la injerencia en los derechos a la vida privada y familiar y al respeto de los datos de carácter personal. Así, por ejemplo, en el asunto *Privacy International*,[51]el TJUE reconoce que el Derecho de la Unión se opone a una normativa nacional que permite a una autoridad estatal obligar a los proveedores de servicios de comunicaciones electrónicas a realizar una transmisión generalizada e indiferenciada de datos de tráfico y de datos de localización a las agencias de seguridad e inteligencia con el fin de proteger la seguridad nacional.[52]

En el asunto *Digital Rights Ireland Ltd*.,[53] el Tribunal detalla claramente los pasos que sigue para determinar si existe o no una injerencia en los derechos reconocidos en la CDFUE. En este caso, la Directiva 2006/24/CE preveía "la obligación de los proveedores de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones de conservar determinados datos generados o tratados por dichos proveedores".[54]

El Tribunal, para estudiar la conformidad de dicha obligación con el Derecho de la Unión sigue las siguientes pautas. Tras concluir a la procedencia del examen de la validez de la Directiva en relación con los artículos 7 y 8 de la CDFUE,[55] el TJUE reconoce la existencia de una injerencia en dichos derechos.[56] A continuación, se pronuncia sobre la justificación de la misma. A estos efectos, por un lado, analiza, si se ha vulnerado el contenido esencial de los derechos, y concluye que no ha habido tal vulneración.[57] Por otro lado, considera que la Directiva 2006/24/CE sí responde a un objetivo de interés general. Efectivamente, la conservación de datos para su eventual acceso por las autoridades nacionales competentes permite prevenir los delitos y luchar contra la delincuencia grave/organizada, contribuyendo a la seguridad

[49] Artículos 13, apartado 2, 15, apartado 1, y 16, apartado 4 de la Directiva (UE) 2016/680.
[50] Artículo 23 del Reglamento (UE) 2016/679.
[51] STJUE, Privacy International, *cit*.
[52] *Ibidem*, párr. 82. Según el TJUE, cuando el *spyware* se despliega activamente por los proveedores de servicios o con su ayuda, se aplicará el Derecho de la Unión (aunque el artículo 4.2 TUE reconozca la competencia exclusiva de los Estados miembros en materia de seguridad nacional) y, por el contrario, cuando los Estados miembros aplican directamente medidas que suponen excepciones a la confidencialidad de las comunicaciones electrónicas, sin imponer obligaciones de tratamiento a los proveedores de servicios de tales comunicaciones, la protección de los datos de las personas afectadas no estará regulada por el Derecho de la Unión (párrs. 30 y ss).
[53] STJUE, Digital Rights Ireland Ltd, *cit.*
[54] *Ibidem*, párr. 16.
[55] *Ibidem*, párrs. 24 a 31.
[56] *Ibidem*, párrs. 32 a 36.
[57] *Ibidem*, párrs. 39 y 40.

pública.[58] Finalmente, realiza el correspondiente control de proporcionalidad, afirmando que la medida que se impugna es adecuada.

Sin embargo, la medida de conservación que la Directive 2006/24 prevé no se puede justificar sólo en base a este objetivo de interés general.[59] A estos efectos, el Tribunal concluye que (a) esta obligación establecida por la Directiva no tiene carácter estrictamente necesario[60] y no establece reglas claras y precisas respecto al alcance de dicha injerencia en los derechos fundamentales,[61] (b) la Directiva tampoco contiene garantías suficientes para velar por la protección de los datos conservados contra los abusos y el acceso y utilización ilícitos de dichos datos,[62] y finalmente (c) el control que se debería realizar para asegurar la máxima protección de los derechos no está garantizado por una autoridad independiente.[63]

En el asunto *La Quadrature du Net,*[64] el TJUE considera que el Derecho de la Unión se opone a "medidas legislativas que establezcan (…), con carácter preventivo, una conservación generalizada e indiferenciada de los datos de tráfico y de localización".[65] Sin embargo, el Derecho de la Unión no se opone a otras medidas legislativas enumeradas por el propio TEDH, siempre que se adopten en situaciones de "amenaza grave para la seguridad nacional que resulte real y actual o previsible"[66] o que se prevean "a efectos de la protección de la seguridad nacional, de la lucha contra la delincuencia grave y de la prevención de las amenazas graves contra la seguridad pública".[67] Además, esas medidas se deben someter a "un control efectivo bien por un órgano jurisdiccional, bien por una entidad administrativa independiente, cuya decisión tenga carácter vinculante".[68]

Finalmente, en relación con la existencia de un control *ex post* de las medidas, el TJUE, en el *asunto Schrems I*, reconoce que una normativa que no prevé posibilidad alguna de que el justiciable ejerza acciones en Derecho para acceder a los datos personales que le conciernen o para obtener su rectificación o supresión no respeta el contenido esencial del derecho fundamental a la tutela judicial efectiva que reconoce el artículo 47 de la Carta.[69] De ahí que es necesario que este control jurisdiccional efectivo exista, y si no fuera el caso se podría vulnerar dicho artículo.

[58] *Ibidem*, párrs. 41 a 44.
[59] *Ibidem*, párr. 51.
[60] *Ibidem*, párrs. 57 a 64.
[61] *Ibidem*, párr. 65.
[62] *Ibidem*, párrs. 66 y 67.
[63] *Ibidem*, párr. 68.
[64] STJUE, La Quadrature du Net, (asuntos acumulados C-511/18, C-512/18 y C-520/18) 6 de octubre de 2020, ECLI:EU:C:2020:791.
[65] *Ibidem*, párr. 168.
[66] *Ibidem*, párrs. 168 y 192.
[67] *Ibidem*, párr. 168.
[68] *Ibidem*, párrs. 139 y 179.
[69] STJUE, Schrems I (asunto C-362/14), 6 de octubre de 2015, ECLI:EU:C:2015:650, párr. 95.

3.2.1.3. Las conclusiones del Parlamento Europeo: acotar el concepto de seguridad nacional

En su recomendación de 15 de junio de 2023,[70] tras la investigación realizada por la Comisión PEGA, el Parlamento europeo recalcó la necesidad de acotar el concepto de seguridad nacional,[71] pues "una mera referencia a la seguridad nacional no puede interpretarse como una excepción ilimitada de la aplicación de la legislación de la UE".[72] A estos efectos, resaltó que los motivos de seguridad nacional que permiten justificar el uso de programas espía siempre deberán respetar "los principios de proporcionalidad, necesidad, legitimidad, legalidad y adecuación (…)".[73] Además, dicha justificación deberá ser de fácil acceso y estar a disposición de un "organismo nacional de control"[74] competente para evaluarla.

En la misma recomendación, el Parlamento Europea considera que los Estados miembros han fracasado en su objetivo de garantizar la protección de los ciudadanos, ya sea porque eran incapaces de hacerlo o porque se negaron a hacerlo.[75] Dada esta falta de protección, se necesita "una acción a escala de la Unión a fin de garantizar que se aplica la letra de los Tratados y se cumple la legislación de la Unión".[76] Sin embargo, en Derecho de la Unión una recomendación expresa un desiderátum, lo que significa que ésta no será, en ningún caso, vinculante (Linde, 2019).

3.2.2. En el ámbito del Consejo de Europa

3.2.2.1. La normativa aplicable

Milione (2020) afirma acertadamente que, en el marco del Consejo de Europa, la seguridad es un "supuesto limitador del ejercicio de determinados derechos humanos en el CEDH". Efectivamente, el CEDH prevé los motivos por los cuales se podrá justificar una vulneración del artículo 8, así como de los demás artículos posiblemente vulnerados por Pegasus.[77] De ahí que podrá haber una injerencia de los Estados parte en dichos derechos, siempre que 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

[70] Recomendación del Parlamento Europeo, de 15 de junio de 2023, al Consejo y a la Comisión a raíz del examen de las alegaciones de infracción y de mala administración en la aplicación del Derecho de la Unión en relación con el uso del programa espía de vigilancia Pegasus y otros programas equivalentes (2023/2500(RSP))'.

[71] El estudio del concepto de 'seguridad nacional' constituye un punto de investigación, sin duda, relevante, que se investigará a lo largo de futuras investigaciones.

[72] Recomendación del Parlamento Europeo, de 15 de junio de 2023, al Consejo y a la Comisión, *cit*., párr. 42.

[73] *Ibidem*, párr. 46.

[74] *Ibidem.*

[75] *Ibidem*, párr. 26.

[76] *Ibidem*.

[77] Véanse los artículos 9, apartado 2, 10, apartado 2, y 11, apartado 2, CEDH.

infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.[78]

3.2.2.2. La jurisprudencia pertinente

Aparte de esta escueta normativa, el TEDH ha establecido una jurisprudencia muy completa al respecto y afirma que la noción de "prevista por ley" exige que la medida impugnada tenga algún fundamento en el Derecho interno. También se refiere a la calidad del Derecho en cuestión, exigiendo que sea accesible a la persona interesada, quien, además, debe poder prever las consecuencias [de dicha medida] sobre ella, y que sea compatible con el Estado de Derecho.[79]

Además, se puede hacer hincapié en que el TEDH ha ido vinculando el principio de proporcionalidad con "las necesidades de una sociedad democrática", las cuales pueden justificar la injerencia en los derechos del CEDH. En este sentido, Gámez (2022) afirma que el TEDH reconoce un amplio margen de apreciación a los Estados parte.[80] Sin embargo, éste no se debe confundir con un poder arbitrario o ilimitado[81] y, por lo tanto, "va acompañado de un control europeo tanto de la ley como de las decisiones que la aplican".[82]

Así, para controlar la necesidad, en una sociedad democrática, de una posible medida de vigilancia secreta, el TEDH considera que hay que examinar sucesivamente (a) la accesibilidad de la normativa interna; (b) el alcance de las medidas de vigilancia secreta; (c) la duración de dichas medidas; (d) los procedimientos que hay que seguir para la conservación, consulta, examen, uso, comunicación y destrucción de los datos interceptados; (e) los procedimientos de autorización; (f) las modalidades de control de la aplicación de esas medidas; y (g) la posible existencia de un mecanismo de notificación, así como los recursos previstos en derecho interno.[83]

El TEDH también clarifica que el control de dichas medidas se puede realizar en tres niveles, es decir (a) cuando se autoriza la medida de intervención (control *ex ante*), (b) mientras se desarrolla (monitorización judicial de la intervención) y (c) cuando cesa (control *ex post*).[84] En relación con las dos primeras fases, es necesario que se ejerzan la vigilancia y el correspondiente control sin el conocimiento del interesado. Esto explica por qué es "indispensable que los procedimientos existentes proporcionen

[78] Artículo 8, apartado 2, CEDH. En los demás artículos, la redacción del segundo apartado difiere, pero su substancia sigue siendo semejante a la del primero. Por tanto, la autora de este trabajo ha decidido reproducir únicamente éste.
[79] STEDH, Weber and Saravia v. Germany no. 54934/00, párr. 84.
[80] *Ibidem*. Véanse también SSTEDH Klass and others v. Germany no. 5029/71, párr. 49 y Roman Zakharov v. Russia no. 47143/06, párr. 232
[81] Véase asunto Klass and others v. Germany, cit., párr. 49
[82] STEDH, Roman Zakharov v. Russia, *cit*., párr. 232.
[83] *Ibidem*, párrs. 236 y ss. Véanse también SSTEDH Big Brother Watch and others v. The United Kindgom no. 58170/13, 62322/14361 y 24960/15, párr. 361 y Centrum för Rättvisa v. Sweden no. 35252/08, párr. 275.
[84] STEDH, Klass and others v. Germany, *cit*., párr. 55.

en sí las garantías apropiadas y equivalentes para la salvaguarda de los derechos del individuo".[85]

Respecto del control a priori (*ex ante*), el Tribunal establece que se debe atribuir preferentemente al poder judicial, pero atribuirlo a otra persona que un juez no vulnera necesariamente los límites de una sociedad democrática. Por lo tanto, dicho control también se puede efectuar por funcionarios o mediante un control político, siempre que sea conforme con el requisito de la independencia y que permita informar de manera objetiva.[86] Además, en el asunto *Szabó and Vissy v. Hungary*, el TEDH considera que por la naturaleza de las amenazas terroristas de hoy en día, se pueden dar situaciones de emergencia en las que la necesidad de obtener una autorización judicial preceptiva no sería viable, sino que sería contraproducente o que incluso haría perder un tiempo valioso.[87]

Ahora, en relación con el control a posteriori (*ex post*), el Tribunal reconoce que debe existir tanto en los casos que afecten a una persona de manera individual, como en los casos que afecten a varias personas de manera generalizada. Además, deberá ser externo y preferentemente judicial.[88] La cuestión de la existencia de un control *ex post* conlleva la pregunta de la notificación de dicha medida una vez haya cesado. Efectivamente, si cuando se haya puesto fin a la medida no se lo notifica a la persona que fue sometida a la misma, ella no podrá ejercer su derecho a un recurso efectivo.[89] Por lo tanto, una vez levantada la vigilancia, la persona afectada deberá ser informada siempre que dicha notificación pueda ser dada sin comprometer la finalidad de la medida de vigilancia que corresponda.[90]

4. CONCLUSIÓN

A lo largo de estos últimos años se ha destapado, mediante diversas investigaciones, el uso abusivo que los Estados del mundo han hecho de Pegasus. Efectivamente, ha quedado acreditado que éste se ha utilizado por varios Estados europeos para fines muy distintos a la lucha contra delitos graves y actos terroristas, es decir, para espiar, entre otras personas, a políticos de la oposición, defensores de los derechos humanos y periodistas. En este sentido, fueron varios los Estados miembros de la UE que utilizaron el programa Pegasus para fines distintos a los amparados por el derecho. Por ejemplo, ha sido el caso de España, en el llamado *CatalanGate*; así como de Polonia, Hungría, Grecia y Chipre.

A raíz de dichas revelaciones, se constituyó la Comisión PEGA del Parlamento Europeo, que se encargó de investigar el uso de Pegasus y otros programas

[85] *Ibidem*.
[86] *Ibidem*, párr. 56.
[87] STEDH, Szabó and Vissy v. Hungary, *cit.*, párr. 80.
[88] *Ibidem*, *cit.*, párr. 79.
[89] Dicho derecho está recogido en el artículo 13 CEDH.
[90] STEDH, Klass and others v. Germany, *cit.*, párr. 58.

equivalentes. Publicó varios informes, subrayando los comportamientos de los Estados de la UE respecto a estos programas. En base a este trabajo de investigación, el Parlamento Europeo adoptó una recomendación sobre el uso de los mismos. Otras investigaciones, por ejemplo, del Consejo de Europa, así como del SEPD, también fueron llevadas a cabo y de todas se desprende que el solo hecho de acceder a los dispositivos de las personas usando un programa espía constituye una injerencia en una multitud de derechos fundamentales. En especial, en los derechos a la vida privada y familiar y a la protección de datos de carácter personal.

Esos derechos, que están protegidos en Europa por la CDFUE y el CEDH, no son absolutos, lo que significa que pueden verse limitados. Sin embargo, para justificar dicha injerencia es necesario que los Estados respeten una serie de requisitos establecidos, tanto en la normativa de la UE y del Consejo de Europa, como en su respectiva jurisprudencia. Así, por ejemplo, el TEDH exige de los Estados parte en el Convenio que respeten una serie de criterios para poder hacer un uso legal de una medida de vigilancia secreta, como lo es Pegasus. A estos efectos, y respecto del llamado *Catalangate*, se podrá, con base en este trabajo, ampliar la investigación para determinar si la legislación española de interceptación de las comunicaciones se adecúa con los requisitos establecidos por este Tribunal. El TJUE también establece algunos requisitos que podrán complementar el estudio de dicha legislación.

En caso de no conformarse con dichas condiciones, las personas víctimas de esa injerencia en sus derechos podrán acudir a distintas vías nacionales, así como europeas e internacionales. De ahí que este trabajo se podrá complementar con un estudio de las vías de acción para luchar, a nivel europeo e internacional, contra el uso abusivo de estos programas espía y la consecuente vulneración de los derechos fundamentales. En el ámbito del Consejo de Europa se podría acudir al TEDH, presentando una demanda individual. Respecto al sistema de protección de derechos humanos disponible en la UE sólo estarán disponibles vías de acción sometidas a la discrecionalidad, bien del juez nacional (cuestión prejudicial), bien de la Comisión Europea (denuncia por infracción del derecho de la Unión). Por lo tanto, estudios posteriores también podrán abordar las futuras sentencias del TEDH sobre el tema, e incluso las futuras sentencias del TJUE, respondiendo a cuestiones prejudiciales y/o posibles procedimientos de infracción puestos en marcha por la Comisión Europea.

5. REFERENCIAS

5.1. Bibliografía

Al-Maskati, M. (et al.) (2022). *Peace through Pegasus: Jordanian Human Rights Defenders and Journalists Hacked with Pegasus Spyware', Joint investigation between Front Line Defenders and Citizen Lab.* https://www.frontlinedefenders.org/sites/default/files/jordanpegasusreport.pdf

Álvarez, V. (2022, 29 de abril). *Pegasus: El escándalo del espionaje masivo*. Amnistía Internacional. https://www.es.amnesty.org/en-que-estamos/blog/historia/articulo/pegasus-espionaje-masivo/

Amnesty International (2021, 19 de julio). *Le Projet Pegasus: des fuites massives de données révèlent que le logiciel espion israélien de NSO Group est utilisé contre des militant·e·s, des journalistes et des dirigeant·e·s politiques partout dans le monde*. https://www.amnesty.org/fr/latest/news/2021/07/the-pegasus-project/

Bouchenni, N. y Gay-Padoan, L. (2022, 10 de mayo). *Pegasus: mode d'emploi du logiciel pirate d'espionnage*. TV5 Monde. https://information.tv5monde.com/international/pegasus-mode-demploi-du-logiciel-pirate-despionnage-395166

Chmielarz, K. (2022). La seguridad nacional y las actividades de vigilancia de los servicios secretos polacos en el contexto del derecho a la privacidad. *Vox Juris*, *40*(1), p. 92 a 100. https://dialnet.unirioja.es/servlet/articulo?codigo=8074477

Citizen Lab (2023, 23 de diciembre). *¿Harías Clic?.* https://catalonia.citizenlab.ca/es/

Encabo, M. A. (2012). *Derechos de la personalidad*. Marcial Pons.

Gámez, N. (2022). Principio de precaución, proporcionalidad y evaluación ex ante y ex post de las normas jurídicas. El caso del lobo ibérico', *Revista de la Administración Pública*, *218.* https://doi.org/10.18042/cepc/rap.218.08

González-Ares, J. A. (2021). Seguridad, libertad y democracia. En Fernández Rodríguez, J. J. (coord.), *Democracia y seguridad respuesta para avanzar en el sistema pública*, Tirant lo Blanch.

Hernández, R. (et al.) (2019). Análisis ético de la información en el escándalo Pegasus. *RITI Journal*, *7*(14). https://dialnet.unirioja.es/descarga/articulo/7237676.pdf

Linde, E. (2019). Las fuentes del Derecho de la Unión Europea. En: CELMA, P. (coord.). *Derecho de la Unión Europea*, Tirant lo Blanch, págs. 188 a 222.

Marzocchi, O. & Mazzini, M. (2022). *Pegasus and surveillance spyware*. European Parliament. https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf

Milione, C. (2015). *El derecho a la tutela judicial efectiva en la jurisprudencia del Tribunal Europeo de Derechos Humanos*. Tirant lo Blanch.

Milione, C. (2020). La noción de seguridad en la doctrina del Tribunal Europeo de Derechos Humanos: referencias al derecho a la tutela judicial efectiva. *Revista de Derecho Político*, 107, enero-abril 2020. https://dialnet.unirioja.es/servlet/articulo?codigo=7326067

NSO Group (2021). Transparency and Responsibility Report. https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf

Orovio, I. y Saura. G. (2022, 14 de mayo). *Quién es quién entre los 18 independentistas espiados por el CNI*. La Vanguardia. https://www.lavanguardia.com/politica/20220514/8265950/personas-espiadas-cni-independentismo-pegasus.html

Rallo, A. (2017). De la "libertad informática" a la constitucionalización de nuevos derechos digitales (1978-2018). *Revista de Derecho Político*, *100.* https://revistas.uned.es/index.php/derechopolitico/article/view/20713/17212

Rebollo, L. (2008). *Vida privada y protección de datos en la Unión Europea*. Dykinson.

Rueckert, P. (2021, 18 de julio). *Pegasus: the new global weapon for silencing journalists*. Forbidden Stories. https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/

Santos. M.J. (2020). Tratamiento de datos, sujetos implicados, responsabilidad proactiva. En: GONZÁLEZ, I. (coord.). *Protección de datos personales*. Tirant lo Blanch.

Scott-Railton, J. (et al.) (2022). *CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru'*. The Citizen Lab, research report #155. https://tspace.library.utoronto.ca/bitstream/1807/119418/1/Report_155--catalangate_012023_.pdf

Stamouli, N. (2022, 5 de noviembre). *Greece's spyware scandal expands further.* Politico. https://www.politico.eu/article/greece-spyware-scandal-cybersecurity/

Tomás, B. (2015). Privacidad versus seguridad en el ámbito europeo'. En: Fayos, A. (coord.). *Los derechos a la intimidad y a la privacidad en el siglo XXI*, Dykinson, Madrid, 2015, págs. 215-241.

Tomás, N. (2022, 5 de mayo). *Spain's CNI admits spying on Aragonès and on Puigdemont's circle, with court approval*. El National.cat. https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html

Verseck, K. (2022, 29 de enero). *Hungarian journalists sue state over Pegasus spyware*. DW. https://www.dw.com/en/pegasus-scandal-in-hungary-journalists-sue-state-over-spyware/a-60598885

5.2. Jurisprudencia

5.2.1. TEDH

STEDH, Klass and others v. Germany no. 5029/71, 6 de septiembre de 1978

STEDH, Weber and Saravia v. Germany no. 54934/00, 29 de junio de 2006

STEDH, Liberty and others v. The United Kingdom no. 58243/00, 1 de julio de 2008

STEDH, Zakharov v. Russia no. 47143/06, 4 de diciembre de 2015

STEDH, Szabó and Vissy v. Hungary, no. 37138/14, 12 de enero de 2016

STEDH, Big Brother Watch and others v. The United Kindgom no. 58170/13, 62322/14361 y 24960/15, 25 de mayo de 2021

STEDH, Centrum för Rättvisa v. Sweden no. 35252/08, 25 de mayo de 2021

5.2.2. TJUE

Sentencia del Tribunal de Justicia (Gran Sala), de 8 de abril de 2014, Asuntos acumulados C-293/12 y C-594/12. *Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources y otros y Kärntner Landesregierung y otros.*
https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62012CJ0293

Sentencia del Tribunal de Justicia (Gran Sala), de 6 de octubre de 2015, Asunto C-362/14. *Maximillian Schrems contra Data Protection Commissioner*.
https://curia.europa.eu/juris/liste.jsf?language=es&jur=C,T,F&num=C-362/14&td=ALL

Sentencia del Tribunal de Justicia (Gran Sala), de 6 de octubre de 2015, Asunto C-650/13. *Thierry Delvigne contra Commune de Lesparre Médoc y Préfet de la Gironde*.
https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:62013CJ0650

Sentencia del Tribunal de Justicia (Gran Sala), de 21 de diciembre de 2016, Asuntos acumulados C-203/15 y C-698/15). *Tele2 Sverige AB*.
https://curia.europa.eu/juris/document/document.jsf?docid=186492&doclang=ES

Sentencia del Tribunal de Justicia (Gran Sala), de 6 de octubre de 2020, Asuntos acumulados C-511/18, C-512/18 y C-520/18. *La Quadrature du Net y otros contra Premier ministre y otros*. https://curia.europa.eu/juris/liste.jsf?num=C-511/18&language=ES

Sentencia del Tribunal de Justicia (Gran Sala), de 6 de octubre de 2020, Asunto C-623/17. *Privacy International contra Secretary of State for Foreign and Commonwealth Affairs y otros*.
https://curia.europa.eu/juris/liste.jsf?language=es&jur=C%2CT%2CF&num=C-623/17

5.3. Normativa

Carta de los Derechos Fundamentales de la Unión Europea, (2000/C 364/01). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.C .2016.202.01.0389.01.SPA

Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Roma, 4 de noviembre de 1950. https://www.echr.coe.int/documents/d/echr/convention_spa

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg, 28.I.1981. https://rm.coe.int/1680078b37

Decisión del Parlamento Europeo, de 10 de marzo de 2022, sobre la constitución, el objeto de la investigación, las competencias, la composición numérica y la duración del mandato de la Comisión de Investigación encargada de examinar el uso del programa espía de vigilancia Pegasus y otros programas equivalentes (2022/2586(RSO)) https://www.europarl.europa.eu/doceo/document/TA-9-2022-03-10_ES.html#sdocta5

Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:32002L0058

Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE. https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX:32006L0024

Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex:32016L0680

Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg, 10.X.2018. https://rm.coe.int/16808ac918

Recomendación del Parlamento Europeo, de 15 de junio de 2023, al Consejo y a la Comisión a raíz del examen de las alegaciones de infracción y de mala administración en la aplicación del Derecho de la Unión en relación con el uso del programa espía de vigilancia Pegasus y otros programas equivalentes (2023/2500(RSP)). https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_ES.html

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32016R0679

Versiones consolidadas del Tratado de la Unión Europea y del Tratado de Funcionamiento de la Unión Europea. DOUE C202 (7.6.2016). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:C:2016:202:TOC

5.4. Informes

Agencia de los Derechos Fundamentales de la Unión Europea (2020). *Aplicación de la Carta de los Derechos Fundamentales de la Unión Europea en la elaboración de normas y políticas de ámbito nacional. Directrices*. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-charter-guidance_es.pdf

Consejo de Europa (2022). *Report: Pegasus spyware and its impacts on human rights*. https://rm.coe.int/pegasus-spyware-report-en/1680a6f5d8

European Data Prootection Supervisor (2017). Manual para la evaluación de la necesidad de las medidas que limiten el derecho fundamental a la protección de datos de carácter personal. https://www.aepd.es/es/documento/guia-evaluar-necesidad-tratamientos-en-politicas-y-medidas-legislativas.pdf

European Data Protection Supervisor (2019). *Directrices del SEPD para la evaluación de la proporcionalidad de las medidas que limitan los derechos fundamentales a la intimidad y a la protección de los datos personales*. https://www.aepd.es/es/documento/guia-evaluar-proporcionalidad-tratamientos-en-politicas-y-medidas-legislativas.pdf

European Parliament (2022). Draft Report Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance (8 November 2022). https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf

European Parliament (2022). Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware REPORT of the Investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2022/2077(INI)) Rapporteur: Sophie in 't Veld Document of compromises. https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/PEGA/DV/2023/05-08/REPORTcompromises_EN.pdf

Naciones Unidas (2019). *La vigilancia y los derechos humanos Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión*. https://www.ohchr.org/es/documents/reports/surveillance-and-human-rights-report-special-rapporteur-promotion-and-protection

Naciones Unidas (2022, 4 de agosto). *The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights.* https://www.ohchr.org/en/documents/thematic-reports/ahrc5117-right-privacy-digital-age

Tribunal Europeo de Derechos Humanos (2013). *Sécurité nationale et jurisprudence européenne*. https://rm.coe.int/16806ae199