La vigilancia por parte de los servicios de inteligencia: salvaguardias y tutela de los derechos fundamentales en la Unión Europea

Resumen

El artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea garantiza a todas las personas en la Unión Europea (UE) el respeto de la vida privada y familiar, mientras que el artículo 8 garantiza el derecho a la protección de los datos de carácter personal. En él se establece que tales datos deben tratarse de modo leal para fines concretos y se garantiza el derecho de toda persona a acceder a los datos recogidos que le conciernan y a obtener su rectificación. Estipula asimismo que una autoridad independiente debe controlar el cumplimiento de este derecho. El artículo 47 de la Carta garantiza el derecho a una tutela judicial efectiva, incluido el derecho de toda persona a que su causa sea oída equitativa y públicamente dentro de un plazo razonable.

Cuando los medios de comunicación de todo el mundo comenzaron a publicar los «documentos de Snowden» en junio de 2013, se puso de manifiesto la existencia de amplios programas de vigilancia mundial por parte de los servicios de inteligencia. Las revelaciones de Edward Snowden no fueron las primeras en sugerir la existencia de programas de vigilancia de las comunicaciones a gran escala que habían sido establecidos a raíz de los ataques del 11 de septiembre de 2001. Sin embargo, la magnitud de las revelaciones no tiene precedentes y afecta potencialmente a la privacidad de las personas en todo el mundo. La vigilancia ya no solo tiene como objetivo los secretos estatales o comerciales, sino que permite interceptar a gran escala las comunicaciones de las personas. Esto interfiere tanto en el respeto de la vida privada y familiar de las personas como en el derecho a la intimidad y la protección de datos, ambos garantizados en la UE por la Carta de los Derechos Fundamentales de la Unión Europea (en adelante, la «Carta»). Como tales, la UE y sus Estados miembros tienen la obligación de proteger dichos derechos, incluso en el contexto de la vigilancia, y proporcionar a las víctimas vías de recurso para reclamar en el caso de vigilancia ilícita.

«Tal vigilancia masiva e indiferenciada es desproporcionada por naturaleza y constituye una injerencia injustificada en los derechos garantizados por los artículos 7 y 8 de la Carta.»
(TJUE, asunto C-362/14, *Maximillian Schrems contra Data Protection Commissioner*, Conclusiones del Abogado General presentadas el 23 de septiembre de 2015)

Las revelaciones generaron una cadena de reacciones. En la comunidad de inteligencia, en particular entre los organismos especializados responsables de supervisar los servicios de inteligencia, se siguieron analizando las repercusiones de las revelaciones de Snowden a través de consultas específicas e informes especiales. Las instituciones de la UE reaccionaron con contundencia. Tanto la Comisión Europea, como el Consejo de la Unión Europea y el Parlamento Europeo redactaron informes sobre las revelaciones, expresaron su preocupación sobre los programas de vigilancia masiva, pidieron aclaraciones a las autoridades de los Estados Unidos y abogaron por «restablecer la confianza» en las relaciones entre la UE y los EE. UU. A pesar de que es demasiado pronto para evaluar todas las repercusiones de las revelaciones de Snowden, las consultas posteriores a las mismas en algunos Estados miembros de la UE concluyeron que sus actuales marcos jurídicos nacionales exigían una reforma. Esto fue corroborado por la Resolución

del Parlamento Europeo de marzo de 2014 sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE. UU., los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de justicia y asuntos de interior (2013/2188(INI), P7_TA (2014)0230) en la que se presentaba un *Habeas Corpus Digital Europeo.*

«Las revelaciones de Edward Snowden nos han dado la oportunidad de reaccionar. Espero que convirtamos esta reacción en algo positivo y duradero para el próximo mandato del Parlamento: una carta de derechos para la privacidad de la que podamos estar orgullosos»
(Claude Moraes, diputado al Parlamento Europeo, Ponente en la investigación del Parlamento Europeo sobre la Agencia Nacional de Seguridad de los EE. UU., Comunicado de prensa de 12 de marzo de 2014)

Comparativa de los marcos legales de los Estados miembros de la UE en el ámbito de la vigilancia

En abril de 2014, el Parlamento Europeo solicitó a la Agencia de los Derechos Fundamentales de la Unión Europea (FRA) que «lleve a cabo una investigación en profundidad sobre la protección de los derechos fundamentales en el contexto de la vigilancia». La Agencia realizó dicha investigación e identificó los marcos jurídicos de los veintiocho Estados miembros de la UE en materia de vigilancia, ofreciendo una visión general de las normas de derechos fundamentales existentes. Se centró en los mecanismos de supervisión y en las vías de recurso a disposición de las personas que alegan violaciones de su derecho a la vida privada.

La investigación jurídica de la FRA no analiza las técnicas de vigilancia como tales, sino que revisa el modo en que los marcos jurídicos actuales permiten el uso de dichas técnicas y explora el papel fundamental que los órganos especializados juegan en la supervisión de la labor de los servicios de inteligencia. Asimismo, examina en qué medida las garantías pertinentes protegen la intimidad y la protección de datos en los veintiocho Estados miembros de la Unión Europea.

Los «servicios de inteligencia» tienen un mandato externo y se centran en las amenazas externas, mientras que los «servicios de seguridad» poseen un mandato interno y se encargan de las amenazas internas. El informe de la Agencia emplea el término «servicios de inteligencia» como término genérico para ambas actividades.

El presente resumen presenta las principales conclusiones de la investigación de la Agencia, que están publicadas de forma completa en el informe titulado *La vigilancia de los servicios de inteligencia: salvaguardias y tutela de los derechos fundamentales en la UE – Marcos legales en los distintos Estados miembros* (véase Más información).

Recogida y cobertura de los datos

Para esta investigación, la FRA examinó los marcos legales sobre vigilancia en los veintiocho Estados miembros de la UE y analizó la legislación y la normativa sobre derechos fundamentales con el fin de presentar un análisis comparativo de la situación jurídica en relación con la vigilancia en el conjunto de la UE.

Tomando como base las respuestas proporcionadas por Franet, la red de investigación multidisciplinar de la agencia, la FRA recopiló datos e información a través de un trabajo de documentación en los veintiocho Estados miembros de la Unión. Se compiló información adicional a través de intercambios con actores clave, entre los que se incluyen una serie de funcionarios de enlace nacionales de la FRA en los Estados miembros, órganos especializados y expertos individuales. Las conclusiones también se basan en los informes y publicaciones existentes que sirven de apoyo a los legisladores nacionales en el establecimiento de marcos jurídicos para los servicios de inteligencia y su supervisión democrática.

En una fase posterior se publicará un segundo informe socio-jurídico de los dictámenes de la FRA, que estará basado en una investigación empírica y que ampliará las conclusiones aquí presentadas.

Las salvaguardias y la legislación de la UE en materia de derechos fundamentales

«La dura realidad es que el uso de la tecnología de vigilancia a gran escala realmente suprime por completo el derecho a la intimidad de las comunicaciones en Internet.»
(*Naciones Unidas, Ponente especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo (2014)*, Cuarto informe anual presentado a la Asamblea General, *A/69/397 de 23 de septiembre de 2014*)

Todos los Estados miembros de la UE están sujetos a una legislación mínima internacional de derechos humanos desarrollada por Naciones Unidas y de aplicación universal, como la Resolución del Consejo de Derechos Humanos sobre el derecho a la privacidad en la era digital (Doc. A/HRC/28/L.27 de 24 de marzo de 2015). Diversos expertos de Naciones Unidas y órganos creados en virtud de tratados condenaron las prácticas de vigilancia a gran escala tras las revelaciones de Snowden. Las directrices del Consejo de Europa, incluida la jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH), también destacan la existencia de unas normas mínimas. Asimismo, resulta relevante la legislación europea tal como ha sido interpretada por el Tribunal de Justicia de la Unión Europea (TJUE). Por último, en los ámbitos donde solo se aplican directamente determinadas normativas internacionales, distintas de la legislación internacional existente en materia de derechos humanos, también son importantes las medidas de autorregulación y el Derecho indicativo.

El informe se centra en los derechos a la intimidad y a la protección de datos, consagrados en los artículos 7 y 8 de la Carta. El derecho a la protección de datos queda asimismo establecido en el derecho primario y derivado de la UE, el cual garantiza que, en su respectivo ámbito de aplicación, el tratamiento de datos personales se realiza de acuerdo con la ley y únicamente en la medida necesaria para cumplir el fin legítimo perseguido. Dichos derechos se extienden a todas las personas, ya sean ciudadanos de la UE o nacionales de terceros países. Con arreglo al artículo 52, apartado 1, de la Carta, cualquier limitación de este derecho debe ser necesaria y proporcionada, responder efectivamente a objetivos de interés general reconocidos por la Unión, estar establecida por la ley y respetar el contenido esencial de dichos derechos.

A pesar de la existencia de directrices internacionales, no existe una comprensión uniforme del concepto de «seguridad nacional» en toda la UE. Ni la legislación europea ni la jurisprudencia del TJUE definen este concepto, aunque el Tribunal ha declarado que las excepciones a los derechos fundamentales deben interpretarse de forma limitada y estar justificadas.

Esta delimitación poco clara de «seguridad nacional» posee repercusiones en la aplicabilidad de la legislación de la Unión Europea. El artículo 4, apartado 2, del Tratado de la Unión Europea establece que la «seguridad nacional seguirá siendo responsabilidad exclusiva de cada Estado miembro», lo cual no significa que la excepción en la «seguridad nacional» exima completamente de la legislación europea. La interpretación de este concepto en los distintos Estados miembros y el modo en que los programas de vigilancia se llevan a cabo podrán ser evaluados por las instituciones de la UE, en particular por el TJUE.

Tipos de vigilancia: específica y no específica

La investigación de la Agencia examina el modo en que se organiza la vigilancia específica y la no específica con arreglo a los marcos jurídicos de los Estados miembros de la UE.

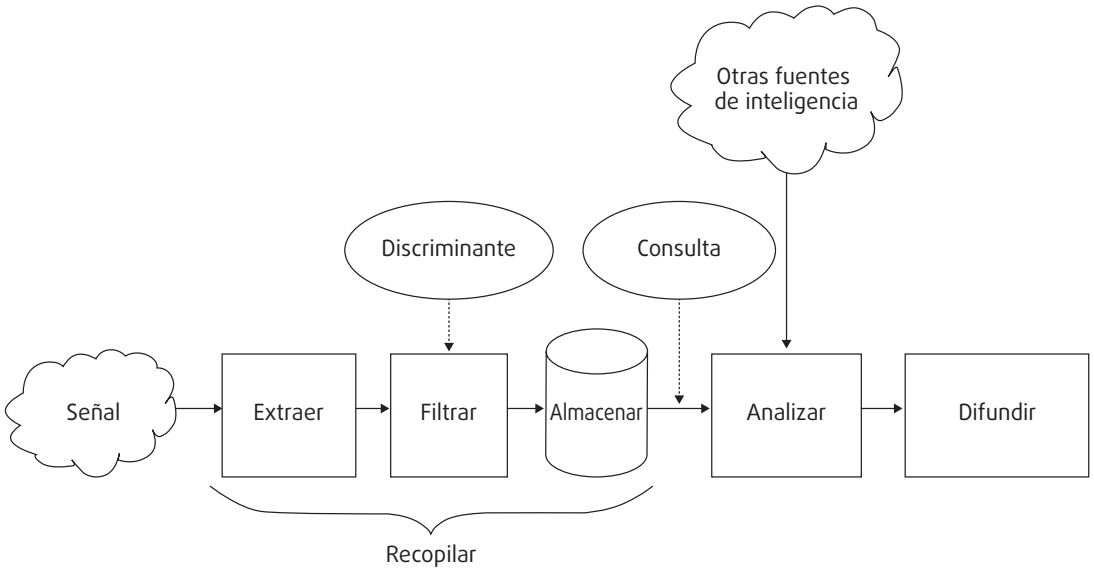
El Comité de Revisión de los Servicios de Inteligencia y Seguridad de los Países Bajos (CTIVD, por sus siglas en neerlandés) define la vigilancia específica y no específica del siguiente modo:

- la intercepción específica hace referencia a una «intercepción en la que puede especificarse de antemano la persona, organización o característica técnica sujeta a la recopilación de datos»;
- la intercepción no específica hace referencia a una «intercepción en la que no puede especificarse de antemano la persona, organización o característica técnica sujeta a la recopilación de datos».

CTIVD, *Informe anual 2013-2014*, La Haya, 31 de marzo de 2014, p. 45 a 46.

La enorme escala de los datos recogidos a través de programas de vigilancia descubierta, como PRISM, Xkeyscore y Upstream, generó reacciones de gran alcance. La «vigilancia masiva» (que suele entenderse como no específica) implica la recopilación de grandes cantidades de datos distintos de los que se

Figura: Modelo conceptual de la inteligencia de señales



Fuente: Estados Unidos, Consejo Nacional de Investigación (2015), p. 28

obtienen con los métodos tradicionales de vigilancia (específica) secreta, como las escuchas telefónicas. Estas últimas están basadas en una sospecha anterior de una persona u organización específica. Este tipo de vigilancia prevalece en los Estados miembros de la UE y está reconocida en sus legislaciones. La gran mayoría de los marcos jurídicos de los Estados miembros de la Unión Europea no regulan o ni siquiera hacen referencia a la «vigilancia masiva» como tal. Solo unos pocos Estados miembros cuentan con legislación detallada sobre inteligencia de señales (SIGINT), que es un término genérico utilizado para describir la intercepción de señales a partir de diversas fuentes por parte de los servicios de inteligencia. La investigación de la Agencia emplea este término a lo largo de su análisis.

La inteligencia de señales procede de la inteligencia militar y hace referencia a la recopilación automática de información a través de la intercepción y la recopilación de datos digitales relacionados con la actividad de inteligencia. La figura siguiente destaca que las señales recopiladas se filtran utilizando discriminantes o selectores (una serie de parámetros utilizados en el proceso de filtrado) ya sea previamente o de forma dinámica, para definir los criterios que determinarán qué datos deben almacenarse para obtener la información pertinente (por ejemplo, «todas las direcciones de correo electrónico utilizadas en las comunicaciones con Yemen»).

El Consejo Nacional de Investigación de las Academias Nacionales de Estados Unidos se refiere a la inteligencia de señales como un término global para cualquier dato almacenado en un dispositivo electrónico. La Comisión de Venecia utiliza SIGINT como un término colectivo para los medios y los métodos de intercepción y de análisis de las comunicaciones de radio (incluida la telefonía móvil y por satélite) y por cable.

El análisis de la Agencia sobre los marcos legales que regulan los métodos de vigilancia de los servicios de inteligencia muestra que la legislación de cinco Estados miembros de la UE (Francia, Alemania, los Países Bajos, Suecia y el Reino Unido) detalla las condiciones que permiten el uso tanto de la vigilancia específica como no específica, así como de la inteligencia de señales. La legislación de otros Estados miembros no especifica de forma suficiente estas condiciones, lo cual obstaculiza un análisis legal de los procedimientos exactos existentes en relación con la recopilación de la inteligencia de señales. A pesar de que la legislación de dichos países no hace referencia específica a SIGINT, esta puede llevarse a cabo igualmente. Sin embargo, dado que en estos países la práctica se prescribe únicamente en medidas reguladoras no publicadas, un análisis de los marcos jurídicos aplicables no ofrecerá ninguna información sobre esta cuestión.

Principales resultados

Servicios de inteligencia y legislación en materia de vigilancia

Objetivo y estructura de los servicios de inteligencia

El principal objetivo de los servicios de inteligencia en las sociedades democráticas es proteger la seguridad nacional y los valores fundamentales de una sociedad abierta, utilizando instrumentos secretos de inteligencia. La organización de la comunidad de inteligencia en los distintos Estados miembros de la UE está estrechamente vinculada a la evolución histórica específica del país y no cumple necesariamente las normas en materia de derechos fundamentales. Como consecuencia, los servicios de inteligencia se establecen de modos muy diversos en toda la Unión Europea. En algunos Estados miembros, dos servicios de inteligencia llevan a cabo esta labor, mientras que en otros, están a cargo de la misma cinco o seis organismos.

- Casi todos los Estados miembros de la Unión Europea han establecido como mínimo dos organismos de servicios de inteligencia distintos, uno para asuntos civiles y otro para asuntos militares. En el presente informe no se abordan estas últimas cuestiones. Los servicios de inteligencia civil están normalmente subordinados a los ministerios de interior y, a veces, también al Primer ministro o al Presidente.

- En algunos Estados miembros, los servicios civiles se subdividen en un servicio con un mandato nacional y otro con un mandato extranjero. Asimismo, algunos Estados miembros han confiado las medidas de inteligencia a unidades especializadas en una amenaza particular, como la delincuencia organizada, la corrupción o la lucha contra el terrorismo.

Protección de la seguridad nacional

La investigación de la Agencia analiza el concepto de «seguridad nacional» a la luz del mandato de los servicios de inteligencia y las medidas de vigilancia que pueden aplicar. De nuevo, las conclusiones revelan una gran diversidad entre los Estados miembros de la UE.

- El principal objetivo de los servicios de inteligencia es proteger la seguridad nacional, aunque el concepto no está armonizado en los Estados miembros de la Unión. El alcance de la seguridad nacional raramente se encuentra definido y algunas veces se emplean términos similares. Algunos Estados miembros no utilizan en absoluto el término «seguridad nacional» sino que, en su lugar, hablan de «seguridad interior» y «seguridad exterior» o de la «seguridad del Estado».

- El alcance de las diversas tareas de los servicios de inteligencia (es decir, su mandato) no es idéntico en todos los Estados miembros de la Unión. Además de los ámbitos más tradicionales, los mandatos de algunos servicios de inteligencia incluyen la delincuencia organizada y la ciberdelincuencia. Estos términos no cuentan con una definición estandarizada.

Regulación legal de la vigilancia

En ocasiones, se desdibuja la línea entre las tareas de los servicios encargados de que se aplique la ley y las tareas de los servicios de inteligencia. Toda ampliación de tareas debe estar debidamente justificada para salvaguardar el Estado, que es la razón subyacente para establecer los servicios de inteligencia.

- La mayoría de los marcos jurídicos de los Estados miembros únicamente regulan la vigilancia específica, ya sea de personas o de organizaciones o grupos definidos. Además de abordar la vigilancia específica, cinco Estados miembros han promulgado leyes pormenorizadas sobre las condiciones de uso de la inteligencia de señales.

- Al observar la normativa de derechos humanos aplicable, se constata que los marcos jurídicos nacionales carecen de definiciones claras que indiquen las categorías de personas y el alcance de las actividades que pueden estar sujetas a la recopilación de información llevada a cabo por la inteligencia.

- Los servicios de inteligencia están regulados por la ley en la gran mayoría de los Estados miembros (en 26 de los 28 Estados miembros). Las disposiciones jurídicas regulan la organización y el funcionamiento de los servicios de inteligencia de los países. La constitución de uno de los Estados miembros prohíbe a sus servicios de inteligencia realizar vigilancias. Otro Estado miembro está en proceso de promulgar una ley que regulará las prácticas de vigilancia de dichos servicios.

- El análisis de la FRA pone de manifiesto que el fundamento jurídico que enmarca el mandato y las competencias de los servicios nacionales de inteligencia en los Estados miembros de la Unión Europea varía desde un único acto jurídico que regula la organización y los medios de los servicios nacionales, hasta complejos marcos compuestos por diversas leyes y ordenanzas que regulan aspectos específicos de su mandato, organización, competencias o medios.

- La mayoría de los Estados miembros organizan la labor de los servicios de inteligencia en dos instrumentos legislativos: uno que hace referencia al mandato y la organización del servicio y otro que cubre los medios de actuación y sus condiciones de uso.

- La mayoría de los Estados miembros de la Unión Europea (23 de 28 Estados) han separado los servicios de inteligencia de las autoridades policiales. Dos Estados miembros han decidido recientemente alejarse de sistemas en los que los servicios de inteligencia dependan de la policía o de cuerpos de seguridad similares.

Supervisión de los servicios de inteligencia

El análisis de la Agencia contempla los mecanismos de responsabilidad relacionados con la vigilancia por parte de los servicios de inteligencia. Dicho análisis describe, en particular, el modo en que los Estados miembros de la Unión Europea han establecido mecanismos de supervisión. La supervisión es una forma de garantizar la responsabilidad pública de las decisiones y las actuaciones de los servicios de inteligencia. Según los expertos, la supervisión pretende evitar el abuso de poder, legitimizar el ejercicio de competencias intrusivas y lograr un mejor resultado tras una evaluación de las actuaciones específicas. El consenso general, que se deriva del informe de la Comisión de Venecia y otros estudios académicos, es que la supervisión debe ser una combinación de:

- control ejecutivo;
- supervisión parlamentaria;
- órganos expertos;
- revisión judicial.

Control ejecutivo y coordinación entre los órganos de supervisión

El órgano ejecutivo puede controlar los servicios de inteligencia de diversos modos: definiendo sus políticas y prioridades estratégicas, estableciendo directrices, mediante el nombramiento o la designación de los altos cargos del servicio, mediante la formulación del presupuesto que el parlamento votará en última instancia, o aprobando la cooperación con otros servicios. El ejecutivo también juega un papel crucial a la hora de autorizar las medidas de vigilancia en algunos Estados miembros.

La supervisión efectiva insta a una coordinación adecuada entre los diversos organismos de supervisión para garantizar que quedan cubiertos todos los aspectos de la labor de los servicios de inteligencia. Si los organismos de supervisión no poseen una comprensión clara y global de la tarea de toda la comunidad nacional de inteligencia, existirán vacíos en la supervisión y se obstaculizará la efectividad del sistema de supervisión en su conjunto.

- La diversidad entre los Estados miembros de la UE en relación con los sistemas políticos y jurídicos se ha traducido en una gran variedad de órganos que supervisan los servicios de inteligencia. Los Estados miembros de la Unión disponen de sistemas de supervisión muy diferentes. Los sistemas existentes permiten extraer buenas prácticas; sin embargo, los ámbitos concretos se beneficiarían de una reforma jurídica que reforzara la función los órganos de supervisión.

- Los distintos órganos de supervisión cuentan con una gran variedad de competencias y también varían sus facultades para ejercer dichas competencias.

- Siete Estados miembros disponen de sistemas de supervisión que combinan órganos expertos, ejecutivos, parlamentarios y judiciales (mediante una aprobación previa). Sin embargo, ninguno de ellos cuenta con un marco jurídico que permita la obtención de datos mediante la inteligencia de señales.

- La supervisión efectiva no exige necesariamente que existan los cuatro tipos de mecanismos de supervisión. Dicha supervisión puede lograrse siempre que los organismos existentes se complementen entre sí y si en su conjunto constituyen un sistema sólido, capaz de valorar si el mandato de los servicios de inteligencia se está llevando a cabo de manera adecuada. Esto es posible si los órganos de supervisión abarcan todos los ámbitos de la actividad del servicio de inteligencia. Sin embargo, en los casos en que el propio mandato no esté claro o suficientemente

detallado, los órganos de supervisión no podrán ejercer su actividad de manera apropiada.

- Es fundamental que los órganos de supervisión tengan acceso a la información y a los documentos. A pesar de que la información recopilada por los servicios de inteligencia es sensible y que debe garantizarse un tratamiento adecuado, los órganos de supervisión no pueden realizar sus tareas sin primero tener acceso a toda la información pertinente. Sin embargo, lo opuesto parece ser la norma.

Supervisión parlamentaria

La supervisión parlamentaria resulta importante dada la responsabilidad que el parlamento posee de exigir responsabilidades al gobierno. El Parlamento, como legislador, es responsable de promulgar una legislación clara y accesible que establezca los servicios de inteligencia y que especifique su organización, las competencias especiales y las limitaciones. También es el encargado de aprobar el presupuesto de dichos servicios y, en algunos Estados miembros, analiza si sus operaciones son conformes al marco jurídico.

- Las conclusiones de la Agencia demuestran que en veinticuatro Estados miembros existe la supervisión parlamentaria, y que veintiuno de ellos disponen de comisiones parlamentarias especiales que supervisan los servicios de inteligencia. Algunos Estados miembros han creado comisiones parlamentarias que tratan los diversos servicios de seguridad e inteligencia, mientras que otros han creado distintas comisiones que tratan los servicios de forma individual.

- No se ha concedido a ninguna comisión parlamentaria de ningún Estado miembro un acceso ilimitado a la información sobre inteligencia.

- Las distintas comisiones parlamentarias de los Estados miembros poseen mandatos diversos: la mayoría tienen competencias de supervisión tradicionales relacionadas con la legislación, el presupuesto y la recepción de información sobre el funcionamiento de los servicios, mientras que solo algunas pueden gestionar las reclamaciones, adoptar resoluciones vinculantes respecto a los servicios de inteligencia o participar en la aprobación de medidas de vigilancia.

- Respecto a la potestad de las comisiones parlamentarias para iniciar investigaciones, la legislación de la mayoría de países autoriza a estas comisiones a solicitar información a los servicios de inteligencia o al órgano ejecutivo, pero no a exigirla.

Supervisión por parte de expertos

La supervisión por parte de expertos tiene un valor excepcional porque permite a las personas que están familiarizadas con la temática, tienen tiempo para dedicarse a esta cuestión y son independientes de las filiaciones políticas, fiscalizar las actuaciones de los servicios de inteligencia. Según el Comisario para los Derechos Humanos del Consejo de Europa, son estos los que tienen una mejor posición para realizar una supervisión diaria de la actividad de los servicios de seguridad e inteligencia.

- A pesar de que la supervisión parlamentaria es crucial, deberá complementarse con la de otros órganos de supervisión, en particular por parte de sólidos órganos expertos que pueden supervisar las actividades operativas, incluida la recopilación, el intercambio y el uso de datos personales, así como la protección del derecho a la vida privada.

- Quince Estados miembros de la UE cuentan con uno o más órganos expertos dedicados exclusivamente a la supervisión de los servicios de inteligencia. Entre las competencias de estos órganos se incluyen la autorización de las medidas de vigilancia, la investigación de denuncias, la solicitud de documentos e información a los servicios de inteligencia, así como asesorar al órgano ejecutivo y al parlamento. Para obtener el máximo potencial, se les deberá conceder la independencia, los recursos y las competencias adecuadas.

- En algunos Estados miembros, las instituciones que son independientes de los servicios de inteligencia y del órgano ejecutivo, no participan en la autorización de medidas de vigilancia.

- En los Estados miembros que cuentan con un órgano independiente para autorizar medidas de vigilancia, la vigilancia específica suele requerir una autorización judicial, mientras que la autorización por parte de órganos expertos es la otra solución preferida. No existe un enfoque común sobre la supervisión de la recopilación de datos mediante la inteligencia de señales.

- A pesar de que es imprescindible conocer los aspectos jurídicos de la vigilancia, los órganos expertos también deben ser competentes en el plano técnico. Algunos Estados miembros garantizan esto al incluir expertos de una gama de ámbitos, incluida las tecnologías de la información y la comunicación (TIC). Otros se basan en gran medida en equipos formados por jueces y parlamentarios en activo o que ya no ejercen.

En los Estados miembros de la UE, se ha concedido un papel fundamental a las autoridades de protección de datos (órganos especializados dedicados a garantizar la intimidad y la protección de datos) a la hora de garantizar los datos personales. Esta función queda consagrada tanto en el derecho primario como en el derecho derivado de la Unión Europea, a pesar de que los órganos expertos encargados de la supervisión de los servicios de inteligencia cuentan sin duda con los conocimientos especializados para proteger la intimidad y los datos en el ámbito de la inteligencia.

- Las conclusiones de la Agencia ponen de manifiesto que, en comparación con otras actividades de tratamiento de datos y los responsables del tratamiento de datos del sector público y privado, las autoridades de protección de datos en siete Estados miembros disponen de las mismas competencias sobre los servicios de inteligencia y sobre los responsables del tratamiento de datos. En doce Estados miembros, las autoridades de protección de datos no tienen competencia sobre los servicios de inteligencia y en nueve sus competencias son limitadas.

- En los Estados miembros en los que las autoridades de protección de datos y otros órganos de supervisión especializados comparten competencias, la falta de cooperación entre estas autoridades puede generar lagunas derivadas de la fragmentación de responsabilidades. En los Estados miembros en los que las autoridades de protección de datos no tienen competencia sobre los servicios de inteligencia, el órgano responsable se encarga de asegurar que se aplican correctamente las salvaguardias en materia de intimidad y de protección de datos.

- La anterior investigación de la Agencia en el ámbito del acceso a las vías de recurso en materia de protección de datos identifica la necesidad de mejorar la capacidad de las autoridades de protección de datos. Esto resulta importante a la vista del papel que dichas autoridades pueden tener a la hora de supervisar los servicios de inteligencia.

Vías de recurso

Con arreglo a las normas internacionales aplicables, toda persona que sospeche ser víctima de una violación de la intimidad y la protección de datos debe tener la posibilidad de interponer un recurso. El derecho a una tutela judicial efectiva, que permita a las personas obtener reparación ante una violación de sus derechos, es un componente esencial del acceso a la justicia. La tutela judicial debe ser «efectiva» en la práctica y en la ley.

Tal como demuestran anteriores informes de la Agencia sobre el acceso a las vías de recurso en materia de protección de datos y sobre el acceso a la justicia, las víctimas de violaciones de la intimidad y de la protección de datos disponen de una serie de vías de recurso. Los órganos extrajudiciales tienen un papel correctivo importante en el ámbito de la vigilancia, dadas las dificultades prácticas a la hora de acceder a los tribunales generales. Los órganos extrajudiciales de los veintiocho Estados miembros incluyen órganos de expertos (incluidas las autoridades de protección de datos), ejecutivos y parlamentarios, así como las instituciones de defensor del pueblo. En algunos Estados miembros, el número de órganos extrajudiciales con funciones de reparación en el ámbito de la vigilancia es relativamente alentador, aunque debe contemplarse a la luz de las siguientes conclusiones.

La complejidad del panorama reparador no facilita la aplicación de la tutela judicial efectiva, ni tampoco lo hace la cantidad de datos recopilados por parte de los servicios de inteligencia que ejecutan SIGINT. La fragmentación y la compartimentación de las distintas vías de recurso dificultan que se exija una reparación. De hecho, los datos recopilados demuestran que, desde las revelaciones de Snowden, únicamente se ha juzgado una serie limitada de casos que impugnan las prácticas de vigilancia en los ámbitos nacionales.

Obligación de informar y el derecho de acceso

El derecho a ser notificado y a acceder a la información resulta crucial para alertar a las personas de las medidas de vigilancia e incoar una acción reparadora. El Tribunal Europeo de Derechos Humanos (TEDH) ha aceptado, no obstante, que tales derechos pueden limitarse de forma justificada (véase la sentencia del TEDH, *Klass y otros contra Alemania*, nº 5029/71, de 6 de septiembre de 1978). Las conclusiones de la Agencia ponen de manifiesto que el secreto que rodea la labor de los servicios de inteligencia limita en efecto estos derechos. Otro factor es la inmensa cantidad de datos recopilados a través de SIGINT, en comparación con formas de vigilancia más tradicionales.

- En ocho Estados miembros, la ley no prevé en absoluto la obligación de informar ni el derecho de acceso. En estos casos, se aplican las normas relativas a los documentos clasificados o a los secretos oficiales. En los otros veinte Estados miembros, la legislación establece la obligación de informar y el derecho de acceso, en algunos casos dentro de plazos específicos, aunque con restricciones. Dichas restricciones incluyen diversos motivos, como la seguridad nacional,

los intereses nacionales o la finalidad de la propia medida de vigilancia.

- Solo dos Estados miembros poseen disposiciones específicas sobre la obligación de informar en el contexto de la inteligencia de señales. En uno, no se informa a las personas si los selectores utilizados no son directamente atribuibles a la persona. En el otro, no se informa a la persona si los datos personales obtenidos se suprimen inmediatamente tras la recopilación y no se tratan posteriormente.

- Los órganos de supervisión de diez Estados miembros de la UE, entre los que se incluyen seis autoridades de protección de datos nacionales, revisan las limitaciones relativas al derecho de ser informado y al derecho de acceder a la información, comprobando si la amenaza a la seguridad nacional invocada es razonable y/o ejerciendo de forma indirecta el derecho de acceso de la persona. En el último caso, los organismos evalúan si puede concederse el acceso a los datos o si es legítimo denegarlo, y analizan la legitimidad del tratamiento de datos. Uno de los Estados miembros requiere una orden judicial que certifique que la notificación obstaculizaría la investigación o que existen argumentos en su contra.

- Otros dos Estados miembros no conceden el derecho de acceso a la información como tal. La legislación, no obstante, establece un derecho que produce el mismo resultado: una persona podrá solicitar al órgano de supervisión que compruebe si sus datos están sujetos a una vigilancia ilegítima.

- En algunos Estados miembros, el órgano de supervisión que ejerce indirectamente el derecho de una persona a solicitar acceso a los datos ni confirma ni niega el tratamiento de datos. Las respuestas se suelen limitar a confirmar que se ha tramitado y/o comprobado la reclamación.

Vías de recurso judiciales

Todos los Estados miembros ofrecen a las personas la posibilidad de denunciar violaciones de la intimidad ante los tribunales, independientemente de si dichas violaciones han tenido lugar mediante inteligencia específica o de señales. Los tribunales establecen una vía para las personas que denuncian una interferencia en su intimidad, que incluye la impugnación de las resoluciones del órgano de supervisión sobre las reclamaciones presentadas. También ofrecen la posibilidad de reparar la situación, incluso en el ámbito de la vigilancia.

- La anterior investigación de la Agencia identificó, no obstante, la falta de especialización de los jueces en materia de protección de datos como un obstáculo grave para una tutela judicial efectiva en el caso de violaciones de protección de datos. Esta conclusión es pertinente para la vigilancia, en la cual, además del secreto necesario vinculado a la inteligencia, resultan fundamentales, por ejemplo, unos conocimientos especializados relevantes en materia de TIC.

- Solo dos Estados miembros han mitigado la falta de especialización en este tipo de recursos designando a jueces y tribunales que posean los conocimientos necesarios para decidir sobre cuestiones (con frecuencia) técnicas, y que tengan autorización para acceder a material secreto.

Recursos extrajudiciales

Las opciones extrajudiciales suelen ser más accesibles para las personas que los mecanismos judiciales, ya que las normas procesales son menos estrictas, es menos costoso presentar una reclamación y los procedimientos son más rápidos. Estudios anteriores de la Agencia confirman este hecho, en particular en el contexto de la protección de datos, puesto que tienden a presentarse más reclamaciones ante las autoridades de protección de datos nacionales y solo unos pocos demandantes inician procedimientos judiciales. Sin embargo, el número de órganos extrajudiciales, distintos de las autoridades de protección de datos, que supuestamente operan en el ámbito de la protección de datos es escaso y muchos de ellos únicamente tienen una competencia limitada para ofrecer vías de recurso.

- Los órganos de supervisión (incluidas las autoridades de protección de datos) encargados de tratar las reclamaciones son instituciones independientes en la gran mayoría de los Estados miembros.

- Cuando un órgano de supervisión ejecutivo tiene facultades para ofrecer vías de recurso, la cuestión de la independencia se plantea cuando dispone, además, de la competencia de asegurar la vigilancia. Los órganos de supervisión parlamentaria y de expertos poseen estructuras administrativas más autónomas, aunque la autonomía no garantiza una tutela judicial efectiva a menos que esté respaldada por conocimientos suficientes. Al evaluar la independencia de un órgano deben considerarse aspectos fundamentales, como el modo en que se nombra a sus miembros y qué lugar ocupan en la jerarquía administrativa.

- Las autoridades de protección de datos de trece Estados miembros de la UE tienen competencia para examinar las reclamaciones de personas y emitir decisiones vinculantes, aunque en tres de ellos, el acceso a los expedientes y las instalaciones es limitada. En cinco Estados miembros se aplican condiciones adicionales, por ejemplo, la presencia del director o de un miembro de la autoridad de protección de datos durante las inspecciones en las instalaciones del servicio de inteligencia.

- Cinco de los siete Estados miembros que confían a sus órganos de supervisión de expertos (distintos de las autoridades de protección de datos) las facultades correctivas específicas, lo hacen permitiendo que estos órganos emitan resoluciones vinculantes. En dos de los Estados miembros de la Unión, el órgano ejecutivo de supervisión también dispone de competencias de reparación. Las comisiones parlamentarias de cuatro Estados miembros están autorizadas a tratar reclamaciones individuales, aunque solo una de ellas puede resolverlas mediante una resolución vinculante.

- Las instituciones de Defensor del Pueblo que existen en los veintiocho Estados miembros tratan mayoritariamente los incumplimientos administrativos en lugar de los verdaderos fundamentos de la vigilancia. Solo un Estado miembro cuenta con una institución del Defensor del Pueblo con facultades correctivas a través de la legislación en materia de inteligencia aplicable. Asimismo, las competencias de las instituciones del Defensor del Pueblo pueden ser bastante limitadas y los procedimientos suelen concluirse con recomendaciones no vinculantes que pretenden ofrecer una solución y orientar las acciones futuras, en lugar de una sentencia vinculante y aplicable. Esto repercute obviamente en la efectividad de las vías de recurso que pueden proporcionar.

- Entre otros elementos que pueden facilitar a las personas el acceso a las vías de recurso se incluyen normas más laxas sobre la carga de la prueba y las acciones de clase, así como la protección efectiva de los denunciantes. La Asamblea Parlamentaria del Consejo de Europa considera que los denunciantes son la herramienta más efectiva para hacer cumplir los límites fijados a la vigilancia.

Conclusiones

Al tratarse de un ámbito en el que la UE tiene competencias limitadas, el informe destaca la diversidad entre los Estados miembros sobre cómo se organizan los servicios de inteligencia y llevan a cabo sus labores esenciales.

Las medidas de vigilancia interfieren en gran medida en los derechos de las personas. Dado su carácter secreto, las personas están obligadas a conceder un grado de confianza al poder público, el cual, a su vez, está obligado a salvaguardar los derechos fundamentales de las personas. Para que la sociedad tenga un grado de confianza hacia sus servicios de inteligencia es necesario que estos rindan cuentas. Una legislación clara y accesible, unos mecanismos de supervisión sólidos, unos mecanismos de control adecuados y una tutela judicial efectiva son solo algunos de los elementos fundamentales para lograr este tipo de rendición de cuentas, que sigue siendo sin duda difícil debido al secreto con el que actúan los servicios de inteligencia. La introducción y el mantenimiento de una legislación clara y accesible y de mecanismos de supervisión sólidos en el Estado miembro constituyen un primer paso hacia un sistema transparente y que respeta los derechos fundamentales. Las dificultades que se han encontrado en este sentido sugieren que siguen existiendo obstáculos.

Las reacciones como consecuencia de las revelaciones de Snowden han subrayado la necesidad de adaptar y reformar los marcos jurídicos pertinentes en la UE y en todos sus Estados miembros. La investigación de la Agencia pone de manifiesto una serie de reformas jurídicas que ya se han llevado a cabo. Las evaluaciones periódicas del funcionamiento y la legitimidad de los marcos que regulan la actividad de los servicios de inteligencia deben formar parte de los sistemas de supervisión. También es una cuestión fundamental el modo en que se siguen reformando los marcos jurídicos que tratan la falta de supervisión adecuada. Asimismo, es necesario que las reformas de los Estados miembros de la UE tengan en cuenta los desarrollos tecnológicos recientes para garantizar que los mecanismos de supervisión disponen de las herramientas necesarias y los conocimientos especializados. Lograr todo esto es, sin duda, complicado aunque vital para llevar a cabo la difícil tarea de proteger la seguridad a la vez que se salvaguardan los derechos fundamentales.

Proteger a los ciudadanos de las amenazas de seguridad y salvaguardar sus derechos fundamentales requiere un delicado equilibrio. Los brutales ataques terroristas y las innovaciones tecnológicas que hacen posible la supervisión de datos de las comunicaciones a gran escala complican aún más esta cuestión, y generan preocupaciones sobre las violaciones de los derechos a la intimidad y a la protección de datos en nombre de la protección de la seguridad nacional. Las revelaciones de Edward Snowden, que pusieron a descubierto unas actividades de vigilancia amplia e indiscriminada en todo el mundo, hacen patente que es necesario mejorar las garantías de dichos derechos.

El presente informe, elaborado en respuesta al llamamiento del Parlamento Europeo de llevar a cabo una investigación profunda sobre la protección de los derechos fundamentales en el contexto de la vigilancia, identifica y analiza los marcos jurídicos existentes en materia de vigilancia en los Estados miembros de la Unión Europea. Al centrarse en la denominada «vigilancia masiva», detalla asimismo los mecanismos de supervisión introducidos en toda la UE, destaca el trabajo de las entidades encargadas de supervisar los esfuerzos de vigilancia y presenta las vías de recurso disponibles para las personas que pretenden impugnar dicha actividad de inteligencia.

El informe expone las complejas consideraciones de la materia y subraya cuán difícil puede ser abordar lo que se suelen considerar prioridades contrapuestas; además contribuye al debate en curso sobre cuál es el mejor modo de reconciliarlas.

Más información:

Para consultar el informe completo de la Agencia – *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Mapping Member States' legal frameworks* (La vigilancia de los servicios de inteligencia: salvaguardias y tutela de los derechos fundamentales en la UE – Marcos legales en los distintos Estados miembros), véase http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services

Véanse asimismo otras publicaciones de la FRA en este ámbito:

- FRA-Consejo de Europa (2014), *Manual de legislación europea en materia de la protección de datos*, Luxemburgo, Oficina de Publicaciones, http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law (disponible en las lenguas de la UE)
- FRA (2014), *Access to data protection remedies in EU Member States* (Acceso a las vías de recurso en materia de protección de datos en los Estados miembros de la Unión Europea), Luxemburgo, Oficina de Publicaciones, http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states y el resumen del informe http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states-summary (disponibles en las lenguas de la UE)

Para más información sobre las actividades de la FRA en materia de protección de datos, véase: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection

Oficina de Publicaciones

FRA – AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA

Schwarzenbergplatz 11 – 1040 Viena – Austria
Tel.: +43 158030-0 – Fax: +43 158030-699
fra.europa.eu – info@fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

Print: ISBN 978-92-9491-032-5, doi:10.2811/413080
PDF: ISBN 978-92-9491-019-6, doi:10.2811/052331

TK-04-15-738-ES-C (print); TK-04-15-738-ES-N (PDF)