ARTÍCULO 29 Grupo «Protección de Datos»

819/14/EN
WP 215

Dictamen 04/2014 sobre la vigilancia de las comunicaciones electrónicas a efectos de inteligencia y seguridad nacional

Adoptado el 10 de abril de 2014

Resumen

Desde el verano de 2013, varios medios internacionales han informado ampliamente sobre las actividades de vigilancia llevadas a cabo por los servicios de inteligencia tanto en los Estados Unidos como en la Unión Europea, basándose sobre todo en la documentación suministrada por Edward Snowden. Estas revelaciones han desencadenado un debate internacional sobre las consecuencias de esta vigilancia a gran escala para la intimidad de los ciudadanos. La manera en que los servicios de inteligencia hacen uso de los datos de nuestras comunicaciones cotidianas, así como del contenido de dichas comunicaciones, subraya la necesidad de fijar límites en lo que respecta al alcance de la vigilancia.

El derecho a la intimidad y a la protección de los datos de carácter personal es un derecho fundamental consagrado en el Pacto Internacional de Derechos Civiles y Políticos, el Convenio Europeo de Derechos Humanos y la Carta de Derechos Fundamentales de la Unión Europea. De ello se deduce que el respeto del Estado de derecho implica necesariamente que este derecho recibe el mayor grado de protección posible.

A partir de este análisis, el Grupo concluye que los programas de vigilancia secretos, masivos e indiscriminados son incompatibles con nuestras leyes fundamentales y no pueden justificarse por motivos de lucha contra el terrorismo u otras importantes amenazas a la seguridad nacional. Las restricciones en los derechos fundamentales de todos los ciudadanos solo pueden ser admisibles si son estrictamente necesarias y proporcionadas en una sociedad democrática.

Esta es la razón por la que el Grupo recomienda varias medidas para que el Estado de derecho quede garantizado y respetado.

En primer lugar, el Grupo pide más transparencia sobre el funcionamiento de los programas de vigilancia. La transparencia contribuye a mejorar y recuperar la confianza entre los ciudadanos y los Gobiernos y las entidades privadas. Esta transparencia implica una mejor información a los ciudadanos en caso de que se deje a los servicios de inteligencia acceder a a sus datos. A fin de informar mejor a los ciudadanos sobre las consecuencias que puede tener la utilización de los servicios de comunicaciones electrónicos en línea y fuera de línea, así como el modo en que se pueden proteger a sí mismos, el Grupo tiene previsto organizar una conferencia sobre la vigilancia en el segundo semestre de 2014, en la que participarán todas las partes interesadas pertinentes.

Además, el Grupo recomienda encarecidamente una supervisión más significativa de las actividades de vigilancia. Una supervisión eficaz e independiente de los servicios de inteligencia, incluido de su tratamiento de los datos personales, es fundamental para garantizar que no se produzcan abusos en esos programas. Por lo tanto, el Grupo considera que una supervisión eficaz e independiente de los servicios de inteligencia supone una participación efectiva de las autoridades de protección de datos.

El Grupo recomienda también la observancia de las obligaciones de los Estados miembros de la UE y de las Partes en el CEDH para proteger los derechos relativos al respeto de la vida privada y a la protección de los datos personales. Además, el Grupo recuerda que los

responsables del tratamiento de datos sujetos a la jurisdicción de la UE deben cumplir el Derecho de la UE vigente aplicable en materia de protección de datos. Asimismo, el Grupo recuerda que las autoridades de protección de datos pueden suspender los flujos de datos y decidir, según su competencia nacional, si conviene imponer sanciones en una situación concreta.

Ni el principio de puerto seguro, ni las cláusulas contractuales tipo, ni las normas corporativas vinculantes pueden servir de base jurídica para justificar la transferencia de datos personales a una autoridad de un tercer país a efectos de vigilancia masiva e indiscriminada. De hecho, las excepciones incluidas en estos instrumentos son de alcance limitado y deben interpretarse de manera restrictiva. Nunca se deben aplicar en detrimento del nivel de protección garantizado por la normativa de la UE y los instrumentos que regulan las transferencias.

El Grupo pide a las instituciones de la UE que concluyan las negociaciones sobre el paquete legislativo de reforma de la protección de datos. También acoge muy positivamente la propuesta del Parlamento Europeo de un nuevo artículo 43 *bis*, que dispone que se informe obligatoriamente a las personas de que se ha permitido el acceso a sus datos por parte de una autoridad pública en los doce últimos meses. La transparencia en relación con estas prácticas aumentará mucho la confianza.

Además, el Grupo considera que el ámbito de la excepción por motivos de seguridad nacional debe aclararse al efecto de proporcionar seguridad jurídica sobre el ámbito de aplicación del Derecho de la UE. Hasta la fecha, ninguna definición clara del concepto de seguridad nacional ha sido adoptada por el poder legislativo europeo, ni existe una jurisprudencia concluyente de los tribunales europeos.

Por último, el Grupo recomienda que se entablen rápidamente las negociaciones de cara a un acuerdo internacional que ofrezca a las personas las salvaguardas adecuadas en materia de protección de datos en caso de ejercicio de actividades de inteligencia. El Grupo también apoya la creación de un instrumento mundial que disponga principios de carácter vinculante y de alto nivel en materia de protección de datos y de la intimidad.

GRUPO DE PROTECCIÓN DE LAS PERSONAS

EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

Creado en virtud de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de

24 de octubre del 1995,

Vistos los artículos 29 y 30, apartado 1, letra c), y apartado 3, de dicha Directiva,

Visto su Reglamento interno, y en particular sus artículos 12 y 14,

HA APROBADO EL SIGUIENTE DICTAMEN:

1. Introducción

Desde el verano de 2013, varios medios internacionales han informado ampliamente sobre las actividades de vigilancia llevadas a cabo por los servicios de inteligencia, tanto en los Estados Unidos como en la Unión Europea (UE) y en otras regiones del mundo, basándose sobre todo en los documentación suministrada por Edward Snowden. Estas revelaciones han desencadenado un debate internacional sobre las consecuencias de esta vigilancia a gran escala para la intimidad de los ciudadanos. También se han planteado dudas sobre hasta dónde podrían llegar legalmente los servicios de inteligencia, tanto en la recogida como en la utilización de la información sobre nuestra vida cotidiana. Este dictamen recoge las conclusiones del análisis jurídico realizado por las autoridades de protección de datos de la UE, reunida en el Grupo del artículo 29 (el Grupo), sobre las repercusiones de los programas de vigilancia para la protección del derecho fundamental a la protección de datos y la intimidad.

La principal tarea de las autoridades de protección de datos es proteger el derecho fundamental a la protección de datos para todas las personas y garantizar el respeto de las disposiciones jurídicas pertinentes por parte de los responsables del tratamiento de datos. Sin embargo, por lo que se refiere a los servicios de inteligencia, muchas autoridades de protección de datos no tienen más que poderes de supervisión limitados, cuando los tienen. Para su supervisión, incluso en lo que respecta al tratamiento de los datos de carácter personal, los Estados miembros han adoptado otras medidas. Por lo tanto, el Grupo ha levantado un inventario de las distintas disposiciones vigentes en la UE en materia de supervisión de los servicios de inteligencia, que se incluyen en el presente dictamen.

El mismo no aborda las hipótesis de interceptación de datos personales por cable. Por el momento, el Grupo no dispone de información suficiente sobre este supuesto para evaluar el régimen jurídico aplicable, ni siquiera a título de hipótesis.

2. Metadatos

Para evaluar el alcance de la posible infracción de las normas de protección de datos, debemos tener claro el problema al que nos enfrentamos. Los funcionarios de la administración pública se refieren a la recogida de metadatos, dando a entender que esto es menos grave que recoger contenidos, pero esto no es así. Los metadatos son todos los datos

sobre una comunicación en curso, excepto el contenido de la conversación. Pueden incluir el número de teléfono o dirección IP de la persona que hace una llamada o envía un correo electrónico, el tiempo y la información relativa a la ubicación, el asunto, el destinatario, etc. Sus análisis pueden revelar datos delicados sobre las personas, debido a las llamadas a determinados números de información médica o centros religiosos, por ejemplo. Como ya falló el Tribunal Europeo de Derechos Humanos en el asunto Malone[1], el tratamiento de metadatos, y la «medición» en este caso, «es un elemento integrante de las comunicaciones por teléfono. En consecuencia, la divulgación de esa información a la policía sin el consentimiento previo del abonado también supone […] una injerencia en un derecho garantizado por el artículo 8». El Tribunal ha mantenido esta posición a lo largo de los años.

También es especialmente importante observar que los metadatos suelen ofrecer información más fácilmente que los propios contenidos de las comunicaciones[2], al ser poderse agregar y analizar con sencillez gracias a su carácter estructurado. Unos complejos instrumentos informáticos permiten analizar grandes conjuntos de datos para identificar modelos y relaciones incorporados, incluidos datos personales, hábitos y comportamientos. No es este el caso de las conversaciones, que pueden desarrollarse en cualquier forma o idioma. Unos complejos instrumentos informáticos permiten analizar grandes conjuntos de datos para identificar modelos y relaciones incorporados, incluidos datos personales, hábitos y comportamientos.

De acuerdo con el artículo 2, letra a), de la Directiva 95/46/CE, los datos personales es «toda información sobre una persona física identificada o identificable (el "interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente». Una definición similar figura en el artículo 2, letra a), del Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal Por lo tanto, a diferencia de lo que ocurre en otros países, los metadatos son datos personales en Europa y, en consecuencia, debe estar protegidos[3].

En la reciente sentencia en los asuntos de conservación de datos, el Tribunal de Justicia de la Unión Europea confirmó que los «datos [de telecomunicaciones], considerados en su conjunto, pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado»[4]. Por último, el Tribunal falló en esa sentencia lo siguiente: «la obligación [...] de conservar durante un determinado período datos relativos a la vida privada de una persona y a sus comunicaciones [...] constituye en sí misma una injerencia en los derechos garantizados por el artículo 7 de la Carta. Además, el acceso de las autoridades nacionales competentes a los datos constituye una injerencia adicional en ese

[1] TEDH, Malone contra Reino Unido, 2 de agosto de 1984.

[2] ACLU contra Clapper, asunto nº 13-3994 (WHP) – Declaración por escrito del profesor Edward W. Felten ante el tribunal de primera instancia del distrito meridional de Nueva York (Estados Unidos).

[3] Se trata de una interpretación tradicional de la legislación sobre la protección de datos. En su Dictamen 4/2007 sobre el concepto de datos personales, el Grupo ya declaró que «también en los casos en que, a primera vista, el alcance de los identificadores disponibles no permita identificar a ninguna persona en concreto, esta puede seguir siendo "identificable", porque esa información, junto con otros datos conservados o no por el responsable del tratamiento de datos, permitirá distinguir a esa persona de otras».

[4] Véase TJCE, asuntos acumulados C-293/12 y C-594/12, 8 de abril de 2014, punto 27.

derecho fundamental. […] La circunstancia de que la conservación de los datos y su posterior utilización se efectúen sin que el abonado o el usuario registrado hayan sido informados de ello puede generar en las personas afectadas el sentimiento de que su vida privada es objeto de una vigilancia constante»[5].

3. Puntos clave

Las revelaciones de Snowden han sido un aldabonazo para muchos. Nunca se había divulgado antes la existencia de tantos diferentes programas de vigilancia gestionados por los servicios de inteligencia y capaces de recoger datos sobre prácticamente todo el mundo. Habían surgido algunos casos antes, pero ahora se aportaban al debate numerosas pruebas sobre su omnipresencia por primera vez. La manera en que los servicios de inteligencia hacen uso de los datos de nuestras comunicaciones cotidianas, así como del contenido de dichas comunicaciones, subraya la necesidad de fijar límites en lo que respecta al alcance de la vigilancia.

Ni siquiera quienes tienen cuidado al llevar sus vidas en línea no se pueden proteger ahora de los programas de vigilancia masiva. Además, teniendo en cuenta los numerosos retos jurídicos, técnicos y prácticos, tampoco las autoridades de protección de datos de todo el mundo pueden prestar una protección satisfactoria. Por lo tanto, se impone un cambio.

En los capítulos siguientes, el Grupo del artículo 29 analiza la recogida masiva de datos por los servicios de inteligencia a la luz de sus programas de vigilancia. Desde el punto de vista jurídico, hay que distinguir entre programas de vigilancia gestionados por los servicios de inteligencia de los Estados miembros y los aplicados por los servicios de inteligencia de terceros países haciendo uso de los datos de los ciudadanos de la UE.

Los programas de vigilancia ejecutados por los Estados miembros de la UE no estarán sujetos en general al Derecho de la UE, dada la excepción de seguridad nacional contemplada en los Tratados europeos, como tampoco lo estarán, por la decisión de los Estados miembros contratantes, varios Reglamentos y Directivas de la UE, incluida la Directiva 95/46/CE sobre la protección de datos. Sin embargo, esto no significa que estos programas solo estén sujetos a la normativa nacional. El análisis realizado por el Grupo del artículo 29 indica que, a pesar de que no sea aplicable el Derecho de la UE, en general, ni la Directiva de protección de datos, en particular, los servicios de inteligencia deberán seguir respetando en su mayor parte, en el ejercicio legal de sus funciones, los principios de protección de datos[6] derivados del Convenio Europeo de Derechos Humanos y del Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Estos principios suelen incluirse también en las constituciones nacionales de los Estados miembros. Los programas de vigilancia basados en una recogida extensa e indiscriminada de datos personales no cumplen en ningún caso los requisitos de necesidad y proporcionalidad establecidos en esos principios de protección de datos. Las limitaciones a los derechos fundamentales deben

[5] Véase TJCE, asuntos acumulados C-293/12 y C-594/12, 8 de abril de 2014, puntos 34, 35 y 37.

[6] Los principios más importantes en materia de protección de datos son los siguientes: tratamiento justo y legal, limitación de la finalidad, necesidad y proporcionalidad, exactitud, transparencia, respeto de los derechos de las personas y adecuada seguridad de los datos.

interpretarse de forma restrictiva, según la jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH)[7] y del Tribunal de Justicia de la Unión Europea (TJUE)[8]. Esto incluye la necesidad de que todas las intrusiones sean necesarias y proporcionadas en relación con el objetivo perseguido. Asimismo, debe tenerse en cuenta que no hay presunción alguna de que el argumento de seguridad nacional esgrimido por una autoridad nacional existe y tiene validez, sino que ello ha de demostrarse.

El Grupo hace hincapié en que es responsabilidad de los Gobiernos de los Estados miembros hacer cumplir todas sus obligaciones nacionales e internacionales, entre ellos el Pacto Internacional de Derechos Civiles y Políticos. De lo contrario, no solo se violarían derechos fundamentales de sus ciudadanos, sino que también quedaría menoscabada la confianza de la sociedad en el Estado de Derecho.

En el caso de los programas de vigilancia gestionados por terceros países, la situación es más compleja. Cuando los datos se recogen, directamente de una fuente situada dentro de la UE o tras una transferencia al tercer país de que se trate (o a otro tercer país), el Derecho de la UE puede seguir siendo aplicable a la divulgación de información obtenida mediante los programas de vigilancia. De hecho, la excepción de seguridad nacional antes mencionada solo se aplica a la seguridad nacional de un Estado miembro de la UE y no a la seguridad nacional de un tercer país. Por supuesto, pueden darse situaciones en las que el interés de seguridad nacional de un tercer país coincida con el de un Estado miembro y en las que puedan estar justificadas las operaciones conjuntas de vigilancia. También en este caso, las autoridades públicas que intervengan en la vigilancia deben ser capaces de demostrar por qué y cómo coinciden los intereses de seguridad nacional de forma que no se aplique el Derecho de la UE.

Se deben observar todas las condiciones aplicables a la transferencia internacional de datos personales establecidas en la Directiva 95/46/CE, lo que significa sobre todo que el destinatario garantice un grado de protección adecuado y que la transferencia se ajuste a la finalidad de la recogida de datos original. Las transferencias también deberán atenerse a la necesidad de contar con la base jurídica adecuada para un tratamiento justo y legal.

Ninguno de los instrumentos disponibles que pueden utilizarse como base alternativa para la transferencia de datos personales a países que no se hayan considerado adecuados (puerto seguro, cláusulas contractuales tipo y normas corporativas vinculantes) permiten a las autoridades públicas de terceros países acceder a los datos personales transferidos sobre la base de estos instrumentos a efectos de una vigilancia indiscriminada y masiva. De hecho, las excepciones contempladas en estos instrumentos tienen un alcance limitado y deben interpretarse de forma restrictiva, es decir, que se utilizarán en casos concretos y para investigaciones específicas. Puesto que los instrumentos de adecuación se han concebido principalmente para ofrecer protección a los datos personales procedentes de la UE, nunca deben aplicarse en detrimento del nivel de protección garantizado por la normativa de la UE y

[7] Véase TEDH, Delcourt, 17 de enero de 1970, y Klass, 6 de septiembre de 1978.

[8] Véase TJCE, asuntos acumulados C-293/12 y C-594/12, 8 de abril de 2014, en los que el Tribunal de Justicia dictamina que la conservación de los datos de tráfico, «sin que se establezca ninguna diferenciación, limitación o excepción», constituye «una injerencia en los derechos fundamentales de gran magnitud y especial gravedad en el ordenamiento jurídico de la Unión, sin que esta injerencia esté regulada de manera precisa por disposiciones que permitan garantizar que se limita efectivamente a lo estrictamente necesario» (puntos 57 y 65).

por los instrumentos que regulan las transferencias. Además, el Grupo señala que, con arreglo a la Directiva de protección de datos, la evaluación del nivel de protección de datos en terceros países en general no comprende el tratamiento de datos con fines policiales o de vigilancia.

Las empresas también deben ser conscientes de que pueden estar infringiendo el Derecho europeo si los servicios de inteligencia de terceros países pueden acceder a los datos de los ciudadanos europeos conservados en sus servidores o si dan cumplimiento a una orden de entregar datos personales a gran escala. A este respecto, las empresas pueden encontrarse en la difícil tesitura de tener que decidir si cumplen o no la orden de facilitar datos personales a gran escala: en cualquier caso infringirán seguramente el Derecho europeo o el de un tercer país. No deben descartarse medidas policiales contra esas empresas si los responsables del tratamiento de datos han cooperado voluntariamente y a sabiendas con los servicios de inteligencia para darles acceso a sus datos. Las empresas aplicarán la mayor transparencia posible y garantizarán que los interesados sepan que, una vez que sus datos personales se transfieren a terceros países que no ofrecen garantías sobre la base de los instrumentos disponibles para estas transferencias, podrían ser sometidos a vigilancia o a derechos de acceso por las autoridades públicas de esos terceros países, en la medida en que tales excepciones estén previstas en los instrumentos mencionados. No obstante, el principal objetivo es encontrar una solución política eficaz. Un acuerdo internacional que ofrezca salvaguardias podría garantizar el respeto de los derechos fundamentales por parte de los servicios de inteligencia.

Con el fin de velar por que los servicios de inteligencia se ajusten en la práctica a los límites impuestos a los programas de vigilancia, hará falta aplicar mecanismos de supervisión significativos en las legislaciones de todos los Estados miembros, que deberían incluir controles completamente independientes de las operaciones de tratamiento de datos por parte de un organismo también independiente, así como poderes ejecutivos efectivos. Además de un control parlamentario eficaz y riguroso, se podría encargar de ello una autoridad de protección de datos u otro organismo independiente apropiado, dependiendo de las disposiciones de supervisión adoptadas por el Estado miembro correspondiente. Si la supervisión la llevara a cabo otro organismo, el Grupo recomienda contactos periódicos entre este organismo y la autoridad nacional de protección de datos para garantizar la aplicación coherente de los principios de protección de datos.

Debe hacerse hincapié en que los mecanismos de supervisión no solo han de existir en teoría, sino que también han de llevarse a la práctica de forma coherente. Las revelaciones de Snowden han mostrado que, si bien existen en teoría muchos controles y contrapoderes, incluido el control judicial de los sistemas previstos de recogida de datos, sigue siendo dudosa la eficacia de la aplicación de esas salvaguardias. Si las salvaguardias contra el acceso indebido no son aplicables a todos los programas de vigilancia ni se aplican a todas las personas, no constituyen lo que el Grupo considera una supervisión significativa.

4. Supervisión de los servicios de inteligencia

Aunque otras entidades han llevado a cabo el año pasado análisis de expertos de las disposiciones de supervisión de los servicios de seguridad e inteligencia de terceros países, no se han realizado tantos de los servicios de inteligencia en cada Estado miembro de la UE. Para obtener una imagen más clara de las diversas disposiciones en Europa en materia de supervisión de los servicios secretos nacionales, el Grupo ha elaborado un cuestionario para todas las autoridades de protección de datos (incluidos dos observadores no pertenecientes a la UE) a fin de conocer sus prácticas nacionales de supervisión a este respecto[9].

Hay dos cuestiones que merecen análisis en particular:

1. La existencia de una supervisión global en el marco jurídico de la seguridad nacional y los servicios de inteligencia.

2. La función, o la falta de función, de la autoridad de control de la protección de datos nacionales en ese marco.

El Grupo de trabajo responde así también a la petición de la vicepresidenta Reding de la Comisión Europea de estudiar cuál podría ser el papel de las autoridades de protección de datos[10].

4.1. Visión de conjunto de los mecanismos nacionales de supervisión

Las actividades de vigilancia examinadas en el presente dictamen y el documento de trabajo adjunto las llevan a cabo principalmente los servicios de inteligencia de acuerdo con su tarea de proteger la seguridad nacional. Hay una amplia diversidad de modelos de supervisión, en función de las tradiciones jurídicas nacionales y de las estructuras dedicadas a las disposiciones de seguridad nacionales. En 26 de los 27 Estados miembros que facilitaron información en respuesta al cuestionario [11] existen servicios de inteligencia, los cuales funcionan sobre la base de una legislación que especifica sus competencias, estructura y responsabilidades. En un Estado miembro no existen servicios de inteligencia y la función de seguridad del Estado la asume una fuerza de policía nacional[12].

La mayoría de los países encuestados informó de la existencia de entre una y tres autoridades de seguridad e inteligencia a escala nacional. En general, existe una división de tareas entre las amenazas para la seguridad interior nacional internas y externas (extranjeros), lo que se traduce en responsabilidades diferentes, civiles (Ministerio del Interior y de Justicia) y militares (Ministerio de Defensa). En tres Estados, las diferentes estructuras están integradas con vistas a crear un sistema de seguridad que informa directamente al jefe de Gobierno (por ejemplo, al primer mMinistro).

[9] Respondieron al cuestionario las autoridades nacionales de protección de datos de 27 Estados miembros, la autoridad subnacional de protección de datos de Sajonia (Alemania) y las autoridades de protección de datos de Suiza y Serbia.
[10] Carta de la vicepresidenta Reding a la presidencia del Grupo del artículo 29, de 30 de agosto de 2013.
[11] Alemania, Austria, Bélgica, Bulgaria, Chequia, Chipre, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Italia, Letonia, Lituania, Luxemburgo, Malta, los Países Bajos, Polonia, Portugal, Rumanía, el Reino Unido y Suecia.
[12] Irlanda.

El tratamiento de los datos personales se basa en una ley nacional del Estado miembro y la supervisión, en la legislación general de protección de datos (en lo sucesivo, «LGPD») o en una o varias leyes especiales que regulan el tratamiento de los datos personales por parte de uno o varios servicios de inteligencia.

4.2. El papel de la autoridad nacional de protección de datos

De la evaluación de la LGPD pertinente se desprende que no se aplica en muchos países a las actividades de los servicios de inteligencia y que la autoridad de protección de datos tiene una función de supervisión limitada e incluso inexistente. La legislación prevé un régimen de protección de datos determinado, pero no contempla necesariamente una supervisión específica por parte de la autoridad de protección de datos.

En los otros dos países no pertenecientes a la UE que han respondido al cuestionario[13], el tratamiento de datos personales por los servicios de inteligencia está regulado por la LGPD y está sujeto a la vigilancia de la autoridad nacional de protección de datos sobre la base de las disposiciones de esa LGPD.

La LGPD, cuando es de aplicación, prevé en general una serie de excepciones (a uno o varios principios) a efectos del tratamiento de datos personales por los servicios de inteligencia. Estas excepciones se refieren normalmente a las tareas básicas de los responsables del tratamiento de datos y de los derechos de los interesados[14]. Las limitaciones pueden referirse a la restricción del derecho a la información y del derecho de acceso del interesado, que ha de ejercerse, en general, a través de la autoridad de control de la protección de datos.

En lo que respecta a la supervisión del tratamiento de datos, parece ser que las leyes nacionales de alcance general en materia de protección de datos (o la ley por la que se establecen los órganos generales de supervisión de la protección de datos) prevén en principio las mismas facultades de supervisión de los servicios de inteligencia que de cualquier otro responsable del tratamiento de los datos únicamente en cuatro Estados miembros[15]. En trece Estados miembros, las competencias de la autoridad de protección de datos incluyen en su ámbito de aplicación los servicios de inteligencia y de seguridad nacional, pero se aplican en algunos casos normas o procedimientos especiales a la supervisión de los servicios de inteligencia, incluida la posibilidad de imponer sanciones[16]. En nueve Estados miembros, la autoridad de protección de datos no tiene facultades de supervisión de los servicios de inteligencia en su calidad de responsables del tratamiento de los datos[17].

Solo en Suecia y Eslovenia existe una supervisión completa por parte de la autoridad de protección de datos en lo referido al cumplimiento de las obligaciones de protección de datos aplicables. En los casos en que otras autoridades nacionales de protección de datos tienen poderes sobre los servicios de inteligencia, las mismas comprueban el cumplimiento de la

[13] Serbia (un servicio civil y dos militares), Suiza (un servicio civil y uno militar).
[14] Por ejemplo, Alemania, Bélgica, Bulgaria, Chipre, Grecia y Hungría. No se ha podido acceder a información sobre las excepciones en el caso de algunos Estados miembros.
[15] Bulgaria, Eslovenia, Hungría y Suecia.
[16] Alemania, Austria, Bélgica, Chipre, Estonia, Finlandia, Francia, Irlanda, Italia, Letonia, Luxemburgo, Polonia y Suecia.
[17] Chequia, Dinamarca, Eslovaquia, España, Malta, los Países Bajos, Portugal, el Reino Unido y Rumanía.

LGPD aplicable y se ocupan de las denuncias y del ejercicio del derecho de acceso por parte de la persona de que se trate. También pueden investigar asuntos, sea por propia iniciativa, sea a instancia de un tercero, y realizar inspecciones sobre el terreno. Pueden existir limitaciones de estos poderes en algunos Estados miembros, por ejemplo, a la hora de imponer el cumplimiento de normas de seguridad especiales al investigar asuntos determinados a fin de tener en cuenta los requisitos del secreto de Estado.

4.3. El papel de otros mecanismos de supervisión independientes

Veinte Estados miembros han declarado que la legislación contempla la supervisión o el control parlamentarios de las actividades de los servicios de inteligencia en paralelo con las competencias de las autoridades de protección de datos en materia de tratamiento de los datos [18], así como sistemas internos de control específicos [19]. Sin embargo, distintas interpretaciones del control parlamentario parecen aplicarse en los Estados miembros y puede considerarse que pocas de las mismas entrañan la existencia de un verdadero organismo responsable de la vigilancia de la protección de datos (incluida la valoración de los derechos de los interesados y el cumplimiento de las disposiciones de la LGPD y de otra legislación específica)[20].

Los sistemas de supervisión existentes son muy diversos e incluyen lo siguiente:

- Una comisión parlamentaria, que puede tener una amplia función de supervisión de las autoridades de inteligencia y seguridad en general o de unos servicios de inteligencia concretos.

- Se ejerce una supervisión o control parlamentarios en colaboración con otros organismos de supervisión independientes que no son la autoridad de protección de datos. Los modelos existentes de control parlamentario adoptan la forma de defensor del pueblo parlamentario, una delegación parlamentaria o una comisión parlamentaria.

- Una comisión parlamentaria es la única autoridad de control fuera de la estructura del poder ejecutivo. Las tareas del Parlamento se formulan en este caso de forma más bien general o de manera que no se contempla el acceso a asuntos abiertos.

- La vigilancia se confía exclusivamente a una autoridad especial. Sin embargo, la legislación sobre protección de datos puede crear la competencia, pero se ha informado también que esta autoridad se regulaba mediante Derecho indicativo hasta hace poco.

- Existe un control judicial especializado junto con la vigilancia parlamentaria general.

[18] Por ejemplo, en Finlandia, el Defensor del Pueblo Parlamentario es responsable junto con la autoridad de protección de datos, pero sus competencias se basan en la legislación específica sobre los servicios de seguridad e inteligencia.
[19] Los veinte Estados miembros a que se hace referencia son los siguientes: Alemania, Austria, Bulgaria, Chequia, Chipre, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Italia, Letonia, Luxemburgo, Polonia, Portugal, el Reino Unido y Rumanía.
[20] El dictamen no analiza la información sobre el control político general y sobre la gestión (ministerial) aportada por las respuestas de varios Estados.

- Existe un control mixto parlamentario y ejecutivo junto con la autoridad de protección de datos general, correspondiendo la presidencia de la comisión especial a un juez, mientras que otros miembros pertenecen a partidos políticos parlamentarios en la actualidad o en el pasado. Existen procedimientos para la celebración de consultas con la autoridad de protección de datos.

- Pueden inspirar mejoras de los elementos de supervisión los sistemas en los que un organismo especial se haya creado específicamente a efectos de la vigilancia sobre los servicios de inteligencia en lo referido a la protección de datos: la Comisión de Supervisión de Datos, formada por tres fiscales nombrados por el fiscal general del Estado, que supervisa los servicios de inteligencia junto con el Consejo de Supervisión parlamentario.

- Aunque pueden someterse asuntos a la autoridad de protección de datos para comprobar si se trata de la seguridad nacional, una vez que se acredite que así se trata, debe remitir el asunto a dos comisarios independientes con una vigilancia judicial independiente sobre los servicios nacionales de inteligencia y la función del secretario de Estado al dictar órdenes de llevar a cabo una vigilancia discreta. En apoyo de todo esto, existe un tribunal específico para las vías de recurso de los interesados.

- Una legislación específica dispone la cooperación entre el organismo especial de vigilancia y la autoridad de protección de datos y un comisario de protección jurídica independiente debe conceder su autorización si los servicios de inteligencia desean llevar a cabo determinadas operaciones (por ejemplo, investigaciones secretas o videovigilancia de personas concretas). Además, la Comisión de Protección Jurídica está obligada a presentar una denuncia ante la autoridad de protección de datos si cree que se han infringido derechos derivados de la LGPD.

La autoridad de protección de datos tiene la facultad de supervisar los servicios de inteligencia, con algunas restricciones, mientras que un órgano parlamentario especial es responsable de supervisar la interceptación de comunicaciones y de tramitar las denuncias. El Comité de Control Parlamentario nombra a los miembros del comité correspondiente. El Presidente debe estar cualificado para ejercer una función judicial.

5. Recomendaciones

A. Mayor transparencia

1. Es necesaria una mayor transparencia sobre el funcionamiento de los programas y sobre lo que hacen y deciden los supervisores

El Grupo considera importante que los Estados miembros sean transparentes en la mayor medida posible sobre su participación en los programas de recogida e intercambio y la recogida de datos de inteligencia, preferiblemente ante el público y, en caso necesario, al menos ante sus Parlamentos nacionales y las autoridades de supervisión competentes. Se recomienda a las autoridades de protección de datos que compartan sus conocimientos técnicos nacionales con el fin de restablecer el equilibrio entre los intereses de la seguridad nacional y el derecho fundamental del respeto de la vida privada de las personas físicas.

Debería existir algún tipo de presentación de informes general sobre las actividades de vigilancia, también en consonancia con la obligación de transparencia que incumbe a los Estados miembros según el Tribunal Europeo de Derechos Humanos [21] . Cualquier interferencia en los derechos fundamentales debe ser previsible y, por lo tanto, estos programas tienen que basarse en una legislación clara, específica y accesible. Se insta a las autoridades nacionales de protección de datos a dar a conocer esta posición a sus Gobiernos.

2. Una mayor transparencia por parte de los responsables del tratamiento de los datos

Las empresas deben aplicar la mayor transparencia posible y garantizar que los interesados sepan que, una vez que sus datos personales se transfieren a terceros países que no ofrecen garantías sobre la base de los instrumentos disponibles para estas transferencias, podrían ser sometidos a vigilancia o a derechos de acceso por las autoridades públicas de esos terceros países, en la medida en que tales excepciones estén previstas en los instrumentos mencionados. El Grupo es consciente de que se puede ordenar a los responsables del tratamiento que se abstengan de informar a los interesados acerca de la orden que hayan recibido de una autoridad pública. También se congratula de los esfuerzos recientes por facilitar a los interesados más y mejor información acerca de las solicitudes que se reciben y anima a las empresas a seguir mejorando las políticas de información.

3. Aumentar al máximo la sensibilización de la población

Los interesados deben estar al corriente de las posibles consecuencias de la utilización de los servicios de comunicaciones electrónicas en línea y fuera de línea y del modo en que pueden protegerse mejor. Se trata de una responsabilidad común de las autoridades de protección de datos, otras autoridades públicas, las empresas y la sociedad civil. Con este fin, el Grupo tiene previsto organizar una conferencia en el segundo semestre de 2014 que reúna a todas las partes interesadas para estudiar un posible planteamiento.

B. Supervisión más significativa

1. Mantener un sistema jurídico coherente para los servicios de inteligencia que incluya normas en materia de protección de datos

Las revelaciones de Snowden han puesto de manifiesto que los servicios de inteligencia de los Estados miembros de la Unión Europea tratan cada día grandes cantidades de datos personales. Estos datos se comparten también con otros servicios de dentro y fuera de la UE. El Grupo considera que es importante que los Estados miembros dispongan de un marco jurídico coherente para los servicios de inteligencia que incluya normas sobre el tratamiento de datos, de conformidad con los principios de protección de datos establecidos en el Derecho europeo e internacional. Los derechos de los interesados deben garantizarse en la mayor medida posible, sin que esto vaya en detrimento de los intereses públicos en juego.

Además, el Grupo recomienda que el Derecho nacional contemple normas claras sobre la cooperación y el intercambio de datos personales con las autoridades policiales para prevenir,

[21] Véase también el Tribunal Europeo de Derechos Humanos en el asunto nº 48135/06 — *Iniciativa de los Jóvenes por los Derechos Humanos contra Serbia* (25 de junio de 2013), p. 6.

combatir y enjuiciar los delitos, así como sobre la transferencia de dichos datos a las autoridades de otros Estados miembros de la UE y de terceros países.

2. Garantizar la supervisión efectiva de los servicios de inteligencia

Debe prestarse especial atención en el Derecho nacional sobre los servicios de inteligencia a los mecanismos de vigilancia existentes. Una vigilancia adecuada, independiente y eficaz reviste la máxima importancia en una sociedad democrática. Por ello, el Grupo considera que las mejores prácticas de los diversos mecanismos de supervisión existentes en la actualidad en los Estados miembros deben formar parte de los mecanismos de control en todos los Estados miembros. Se insta a las autoridades nacionales de protección de datos a aportar los elementos siguientes al debate nacional sobre la supervisión de los servicios de inteligencia:

- unos controles internos fuertes del cumplimiento de la legislación nacional a fin de garantizar la rendición de cuentas y la transparencia;

- un control parlamentario efectivo de acuerdo con las tradiciones legislativas nacionales; las autoridades nacionales de protección de datos debería animar a los Parlamentos que ya tienen poderes de supervisión de los servicios de inteligencia a ejercerlos activamente;

- una vigilancia externa independiente, rigurosa y efectiva ejercida por un organismo especial con la participación de las autoridades de protección de datos o por estas mismas autoridades, con el poder de acceder a los datos y a otra documentación pertinente de forma normal y por iniciativa propia (*ex officio*), así como la obligación de realizar inspecciones a raíz de denuncias; no debe exigirse la aprobación previa de los servicios de inteligencia que deben ser supervisados.

C. Aplicación efectiva de la legislación vigente

1. Observar las obligaciones de los Estados miembros de la UE y de las Partes en el CEDH en materia de protección de los derechos relativos al respeto de la vida privada y a la protección de datos personales

Todos los Estados miembros son Partes en el Convenio Europeo de Derechos Humanos. Por lo tanto, los Estados miembros han de cumplir las condiciones establecidas en el artículo 7 y 8 del CEDH para sus propios programas de vigilancia. Sus obligaciones no acaban ahí. El artículo 1 del CEDH también obliga a las Partes a garantizar los derechos y libertades contemplados en el Convenio para todas las personas sujetas a su jurisdicción. En ambos casos, puede llevarse a los Estados miembros de la UE y a cualquier Parte en el CEDH ante el Tribunal Europeo de Derechos Humanos por la vulneración del derecho de los interesados europeos al respeto de la vida privada.

2. Los responsables del tratamiento de datos sujetos a la jurisdicción de la UE deben cumplir la legislación de protección de datos de la UE

Los responsables del tratamiento de datos establecidos en la UE o que hagan uso de equipos de un Estado miembro tienen que respetar las obligaciones que les incumben en virtud del Derecho de la UE, incluso en el caso de que la legislación de otros países en los que operen

sea contraria al Derecho de la UE. A este respecto, las autoridades de protección de datos no pueden pasar por alto el hecho de que pueden producirse transferencias de datos en contravención del Derecho de la UE. Por consiguiente, el Grupo recuerda que las autoridades de protección de datos pueden suspender, con arreglo a las condiciones establecidas por las disposiciones sobre protección de datos de la UE y nacionales, los flujos de datos previstos en los instrumentos de transferencia en caso de una probabilidad importante de vulneración de los principios de la protección de datos y que la continuación de la transferencia podría dar lugar a un riesgo inminente de perjuicios graves para los interesados. Las autoridades nacionales de protección de datos deberían decidir según su competencia nacional si las sanciones están justificadas en una situación concreta.

D. Mejora de la protección a nivel europeo

1. Adopción del paquete de reformas de la protección de datos

Con el fin de ofrecer una protección de datos rigurosa en Europa, la conclusión de las negociaciones sobre el paquete de reformas de la protección de datos reviste la mayor importancia. El nuevo Reglamento general de protección de datos y la Directiva sobre la protección de datos policiales y judiciales no solo persiguen una mejor protección de los datos personales, sino que también se han formulado para precisar su ámbito de aplicación y conceder más competencias ejecutivas a las autoridades de protección de datos. En particular, la posibilidad de imponer sanciones (financieras), como último recurso, debería garantizar una mayor influencia en los responsables del tratamiento de datos. El Grupo también acoge muy positivamente la propuesta del Parlamento Europeo de prever una notificación obligatoria a las personas cuando se haya permitido el acceso a sus datos por parte de una autoridad pública en los últimos doce meses. La transparencia en relación con estas prácticas aumentará mucho la confianza. Por ello, el Grupo insta al Consejo y al Parlamento Europeo a ajustarse al calendario acordado[22] y a procurar que ambos instrumentos puedan adoptarse a lo largo de 2014.

2. Precisar el ámbito de aplicación de la excepción por motivos de seguridad nacional

En la actualidad, no existe un concepto común de seguridad nacional. Hasta la fecha, ninguna definición clara de la noción de seguridad nacional ha sido adoptada por el poder legislativo europeo, ni existe jurisprudencia concluyente de los tribunales europeos. Sin embargo, esta excepción no debe ampliarse al tratamiento de datos personales para fines para los que no puedan ser legalmente empleados.

Otro aspecto de la cuestión que debe aclararse es la medida en que una exención centrada en la seguridad nacional sigue reflejando la realidad en un momento en que el trabajo de los servicios de inteligencia se confunde cada vez más con el de las autoridades policiales y persigue varios objetivos diferentes. Los datos se comparten sin cesar en todo el mundo, con independencia de si la seguridad del país puede sacar ventaja del análisis de estos datos. Por lo tanto, el Grupo pide al Consejo, a la Comisión y al Parlamento que lleguen a un acuerdo con el fin de definir el principio de seguridad nacional y delimitar de forma concluyente lo

[22] http://euobserver.com/justice/122853

que se debería considerar competencia exclusiva de los Estados miembros. Al definir el principio de seguridad nacional, se ha de tener debidamente en cuenta las reflexiones del Grupo, especialmente las expuestas en el presente dictamen. Las instituciones de la UE también deben aclarar en el paquete legislativo de reformas de la protección de datos que la protección de la seguridad nacional de terceros países no puede por sí sola excluir la aplicabilidad de la legislación de la UE.

E. Protección internacional para los residentes en la UE

1. Insistir en salvaguardias adecuadas en lo relativo a la comunicación de datos de inteligencia

Las autoridades públicas de terceros países, en general, y los servicios de inteligencia, en particular, no deberán tener acceso directo a los datos tratados del sector privado en la UE. Si necesitan acceder a dichos datos en un caso concreto en atención a una sospecha razonable, deberán presentar, en su caso, una solicitud en virtud de los acuerdos internacionales, ofreciendo las oportunas garantías en lo relativo a la protección de datos. En lo que respecta a la comunicación de información de los servicios de inteligencia, los Estados miembros han de velar por que la legislación nacional disponga una base jurídica específica para dichas transferencias, así como unas salvaguardias adecuadas para la protección de los datos personales. En opinión del Grupo, los acuerdos de cooperación secreta entre Estados miembros o terceros países no se ajustan a las normas del TEDH en lo relativo a la existencia de una base jurídica clara y accesible.

2. Negociar acuerdos internacionales a fin de conceder garantías adecuadas de protección de datos

La idea del llamado acuerdo marco, que negocian ahora los Estados Unidos y la UE, es un paso en la dirección correcta. No obstante, es probable que tal acuerdo tenga el defecto de contemplar una excepción relativa a los casos de seguridad nacional, al menos desde la perspectiva de la UE, en la medida en que se negocia como un acuerdo basado únicamente en el Derecho de la UE. Su estructura sugiere que se aplicaría únicamente a los datos transferidos entre las autoridades públicas de los Estados Unidos y de la UE y no a los datos recogidos por entidades privadas, lo que también se desprende del informe del Grupo de contacto de alto nivel UE-Estados Unidos sobre intercambio de datos y protección de los datos personales[23], que constituye la base de las negociaciones sobre el acuerdo marco. El Grupo señala que, de conformidad con el acuerdo marco, la finalidad del tratamiento de los datos transferidos debe ser la misma tanto en la UE como en los Estados Unidos. No sería aceptable si los datos procedentes de la aplicación del Derecho de la UE pudieran utilizarlos posteriormente los servicios de inteligencia a efectos de la seguridad nacional de los Estados Unidos, si tal cosa no es también posible en la UE.

Puesto que el acuerdo marco no será suficiente para ofrecer una protección completa a todos los ciudadanos, lo que se necesita es un acuerdo internacional que proporcione una protección adecuada contra la vigilancia indiscriminada. También se podría paliar el conflicto actual

[23] Documento del Consejo 15851/09, de 23 de noviembre de 2009.

entre jurisdicciones que afecta a una parte de las actividades de vigilancia divulgadas si ese acuerdo fijara unos límites claros a la vigilancia. Sin embargo, tal acuerdo estaría ligado directamente a la excepción por motivos de seguridad nacional y, por lo tanto, quedaría fuera del ámbito de aplicación del Derecho de la UE. En consecuencia, corresponde a los Estados miembros entablar negociaciones de manera coordinada. Debe tenerse debidamente en cuenta la determinación clara de las actividades de vigilancia descritas que estarían cubiertas efectivamente por la seguridad nacional y de aquellas que se relacionan más bien con los fines policiales y de política exterior, aspectos que entrarían en el ámbito de aplicación del Derecho de la Unión. Esto posibilitaría que las instituciones de la UE tuvieran una participación más estrecha, de tomarse medidas en este sentido.

Este nuevo Acuerdo no ha de ser de secreto, sino que debe hacerse público e incluir las obligaciones de las Partes Contratantes sobre la necesaria supervisión de los programas de vigilancia, la transparencia, la igualdad de trato al menos de los ciudadanos de todas las partes en el acuerdo, las vías de recurso y otros derechos en materia de protección de datos. Asimismo, debe alentarse a las partes interesadas a cerciorarse de que sus parlamentos estén puntualmente informados acerca del uso y el valor del acuerdo celebrado.

3. Fomentar un instrumento mundial de protección de la vida privada y de los datos personales

El Grupo apoya la creación de un instrumento mundial vinculante que contemple unos principios de protección de datos y de la intimidad ejecutivos y de alto nivel, tal y como se acordó en la Conferencia Internacional de Autoridades de Protección de Datos y Protección de la Intimidad en su declaración de Madrid[24]. En este sentido, podría estudiarse la adopción de un Protocolo adicional al artículo 17 del Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas. En tal instrumento internacional se debe velar por que las salvaguardias ofrecidas se apliquen a todas las personas afectadas. También es necesario llegar a una interpretación general de lo que se entiende por «tratamiento de datos», ya que existen grandes diferencias en cómo se entiende en todo el mundo.

El Grupo apoya la iniciativa del Gobierno alemán y el llamamiento hecho por la Conferencia Internacional de Autoridades de Protección de Datos y Protección de la Intimidad[25][26], a lo que se añade que sigue respaldando la adhesión de terceros países al Convenio 108 del Consejo de Europa.

[24] Resolución de Madrid relativa a estándares internacionales sobre protección de datos personales y privacidad, adoptada por la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Protección de la Intimidad.
[25] http://www.bundesregierung.de/Content/EN/Artikel/2013/07/2013-07-19-bkin-nsa-sommerpk.html.
[26] Resolución de Varsovia sobre protección en encaje de datos y la protección de la intimidad en el Derecho internacional, adoptada en la 35ª Conferencia Internacional de Autoridades de Protección de Datos y Protección de la Intimidad.