GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29

16/ES
WP 238

Dictamen 01/2016 sobre el proyecto de Decisión sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU.

Adoptado el 13 de abril de 2016

RESUMEN

El 29 de febrero de 2016, la Comisión Europea publicó una Comunicación, un proyecto de Decisión de adecuación con textos anexos que constituyen un nuevo marco para los intercambios transatlánticos de datos personales con fines comerciales: el Escudo de la privacidad Unión Europea-EE. UU. (en lo sucesivo, el Escudo de la privacidad). Con él se pretende sustituir el anterior régimen de puerto seguro de los EE. UU., invalidado por el Tribunal de Justicia de la Unión Europea (en lo sucesivo, el TJUE) el 6 de octubre de 2015 en el asunto Schrems.

De conformidad con el artículo 30, apartado 1, letra c), de la Directiva 95/46/CE, el Grupo de Trabajo sobre protección de datos del artículo 29 (en lo sucesivo, el Grupo de trabajo del artículo 29) evaluó esos documentos con el fin de emitir su dictamen sobre el proyecto de Decisión de adecuación. El Grupo de trabajo del artículo 29 valoró tanto los aspectos comerciales como las posibles excepciones a los principios del Escudo de la privacidad con fines de seguridad nacional, aplicación de la ley e interés público.

El Grupo de trabajo del artículo 29 tuvo en cuenta el marco jurídico aplicable de la UE en materia de protección de datos según lo establecido en la Directiva 95/46/CE, así como los derechos fundamentales al respeto de la vida privada y a la protección de los datos codificados en el artículo 8 del Convenio Europeo de Derechos Humanos y los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea. Asimismo, tomó en consideración el derecho a la tutela judicial efectiva y a un juez imparcial consagrado en el artículo 47 de la Carta, además de la jurisprudencia relativa a los diversos derechos fundamentales.

Por otra parte, el análisis refleja el razonamiento del TJUE en el asunto Schrems, relativo al margen de apreciación de la Comisión en una evaluación de adecuación. La verificación y los controles de los requisitos de adecuación se deben aplicar de manera estricta, teniendo en cuenta los derechos fundamentales al respeto de la vida privada y a la protección de los datos y el número de personas potencialmente afectadas por la transferencia.

El Escudo de la privacidad debe considerarse en el contexto internacional actual, de aparición de los macrodatos y necesidades crecientes en materia de seguridad. El alcance y el ámbito de la recogida y uso de los datos personales han aumentado de manera espectacular desde la Decisión original de puerto seguro de 2000. Las autoridades europeas de protección de datos sostienen categóricamente la importancia de los principios que defienden.

En primer lugar, el Grupo de trabajo del artículo 29 acoge con satisfacción las significativas mejoras introducidas por el Escudo de la privacidad respecto de la Decisión de puerto seguro. Observa que los negociadores han abordado muchas de las deficiencias del puerto seguro que había subrayado en su carta de 10 de abril de 2014 a la Vicepresidenta Reding.

El hecho de que los principios y las garantías previstos por el Escudo de la privacidad figuren tanto en la Decisión de adecuación como en sus anexos hace que la información resulte difícil

de encontrar y, a veces, sea incoherente. Esto contribuye a una falta general de claridad acerca del nuevo marco y a dificultar aún más la accesibilidad para los interesados, las entidades y las autoridades de protección de datos. Por otra parte, el texto adolece de falta de claridad lingüística. Por consiguiente, el Grupo de trabajo del artículo 29 insta a la Comisión a proponer conceptos que resulten claros y comprensibles a ambos lados del Atlántico.

Por lo que se refiere a la legislación aplicable, el Grupo de trabajo del artículo 29 destaca que si la Decisión de adecuación del Escudo de la privacidad se adopta sobre la base de la Directiva 95/46/CE, debe ser coherente con el marco jurídico de la UE de protección de datos, tanto por su ámbito de aplicación como por su terminología. El Grupo de trabajo del artículo 29 considera que se ha de realizar una revisión poco después de la entrada en vigor del Reglamento general de protección de datos, a fin de garantizar la continuidad del mayor nivel de protección de datos ofrecido por el Reglamento en la Decisión de adecuación y sus anexos.

Sobre los aspectos comerciales del Escudo de la privacidad

El objetivo fundamental del Grupo de trabajo del artículo 29 es garantizar que cuando se traten datos personales con arreglo a las disposiciones del Escudo de la privacidad se mantenga un nivel de protección de los particulares básicamente equivalente. Aunque el Grupo de trabajo del artículo 29 no espera que el Escudo de la privacidad sea una mera copia exhaustiva del marco jurídico de la UE, considera que debe contener la sustancia de los principios fundamentales y, por consiguiente, garantizar un nivel de protección «sustancialmente equivalente».

A pesar de las mejoras que brinda el Escudo de la privacidad, el Grupo de trabajo del artículo 29 considera que algunos de los principios clave de la protección de datos tal y como se recogen en la legislación europea no se reflejan en el proyecto de Decisión de adecuación y los anexos, o han sido sustituidos por otros conceptos de manera inadecuada.

Por ejemplo, el principio de conservación de datos no se menciona expresamente y no se puede interpretar claramente a partir de la formulación actual del principio de integridad de los datos y de limitación de la finalidad. Por otra parte, no se menciona en ningún momento la protección que debe reconocerse ante las decisiones individuales automatizadas basadas únicamente en el tratamiento automatizado. La aplicación del principio de limitación de la finalidad al tratamiento de datos tampoco está clara. A fin de aportar una mayor claridad en la utilización de diversos conceptos importantes, el Grupo de trabajo del artículo 29 sugiere que la UE y los EE. UU. acuerden unas definiciones claras y que estas se recojan en un glosario que se integrará en las preguntas frecuentes sobre el Escudo de la privacidad.

Dado que el Escudo de la privacidad también se utilizará para transferir datos fuera de los EE. UU., el Grupo de trabajo del artículo 29 insiste en que las transferencias ulteriores de una entidad del Escudo de la privacidad a terceros países destinatarios deben ofrecer el mismo nivel de protección en todos los aspectos del Escudo (incluida la seguridad nacional) y no deben conducir a reducir o eludir los principios de protección de datos de la UE. Cuando se prevea una transferencia ulterior a un tercer país en el marco del Escudo de la privacidad,

cada organización del Escudo debe tener la obligación de evaluar, antes de la transferencia, los requisitos obligatorios de la legislación nacional del tercer país aplicable al importador de datos. En general, el Grupo de trabajo del artículo 29 considera que el marco en el que se realizan las transferencias ulteriores de datos personales de la UE es insuficiente, en particular en lo que respecta a su alcance, la limitación de su finalidad y las garantías aplicables a las transferencias a agentes.

Por último, aunque el Grupo de trabajo del artículo 29 toma nota de los recursos adicionales que se han puesto a disposición de los individuos para que ejerzan sus derechos, está preocupado porque en la práctica el nuevo mecanismo de recurso pueda resultar demasiado complejo y difícil de utilizar por los ciudadanos de la UE y, por tanto, sea ineficaz. Así pues, se precisan mayores aclaraciones de los distintos procedimientos de recurso; en particular, si lo desean, podría considerarse a las autoridades de protección de datos de la UE como puntos de contacto naturales para los particulares de la UE en los diversos procedimientos, con la posibilidad de actuar en su nombre.

Excepciones por motivos de seguridad nacional

En cuanto al acceso a los datos por las autoridades públicas, tanto en la UE como en terceros países, el Grupo de trabajo del artículo 29 recuerda su análisis de los derechos fundamentales pertinentes contenido en el documento de trabajo sobre la justificación de las injerencias en los derechos fundamentales al respeto de la vida privada y a la protección de los datos a través de medidas de vigilancia a la hora de transferir datos personales (garantías esenciales europeas) (WP237).

Un gran paso adelante desde la Decisión de puerto seguro es que el proyecto de Decisión de adecuación aborda ampliamente el posible acceso a los datos tratados en el marco del Escudo de la privacidad con fines de seguridad nacional y de aplicación de la ley. El Grupo de trabajo del artículo 29 reconoce este importante paso, así como el incremento de la transparencia que ofrece la administración estadounidense sobre la normativa aplicable a la recogida de datos de inteligencia (anexo VI).

El Grupo de trabajo del artículo 29 señala, sin embargo, que las observaciones de la Oficina del Director de Inteligencia Nacional (ODNI, por sus siglas en inglés) no impiden la recogida masiva e indiscriminada de datos personales procedentes de la UE. El Grupo de trabajo del artículo 29 reitera su posición de larga data de que la vigilancia masiva e indiscriminada de las personas físicas no puede considerarse en ningún caso proporcionada y estrictamente necesaria en una sociedad democrática, como exige la protección que ofrecen los derechos fundamentales aplicables. Además, la supervisión global de todos los programas de vigilancia es crucial. El Grupo de trabajo del artículo 29 constata que existe una tendencia a recoger más datos a una escala masiva e indiscriminada a la luz de la lucha contra el terrorismo. Dada la preocupación que ello supone para la protección de los derechos fundamentales al respeto de la vida privada y a la protección de los datos, el Grupo de trabajo del artículo 29 está a la espera de las futuras sentencias del TJUE en los asuntos relativos a la recogida de datos masivos e indiscriminados.

En relación con las posibilidades de recurso, el Grupo de trabajo del artículo 29 acoge con satisfacción la creación de la figura de un Defensor del Pueblo como un nuevo mecanismo a estos defectos. Esto puede constituir una mejora significativa de los derechos de los ciudadanos de la UE en lo que se refiere a las actividades de los servicios de inteligencia de los EE. UU. Sin embargo, al Grupo de trabajo le preocupa que este nuevo organismo no sea lo bastante independiente, no esté investido de poderes adecuados para ejercer eficazmente sus derechos y no garantice, por tanto, una tutela judicial satisfactoria en caso de desacuerdo.

Revisión conjunta

El mecanismo de revisión conjunta anual mencionado en el proyecto de Decisión de adecuación constituye un factor clave para la credibilidad global del Escudo de la privacidad, y el Grupo de trabajo del artículo 29 acoge con gran satisfacción la oportunidad que ello supondría a la hora de revisar la Decisión de adecuación. A este respecto, el Grupo de trabajo del artículo 29 considera que sus representantes nacionales estarán en condiciones de participar plenamente en el proceso de revisión, pero pide que se aclaren las normas concretas. Las modalidades (incluido el informe resultante, su publicidad y sus posibles consecuencias, así como la financiación) se deberán acordar con antelación suficiente a la primera revisión.

Conclusión

El Grupo de trabajo del artículo 29 destaca las grandes mejoras del Escudo de la privacidad con respecto a la Decisión de puerto seguro invalidada. Dadas la preocupación expresada y las aclaraciones solicitadas, el Grupo de trabajo del artículo 29 insta a la Comisión a resolver estas cuestiones, identificar soluciones adecuadas y aportar todas las aclaraciones necesarias para mejorar el proyecto de Decisión de adecuación y velar por que la protección que brinda el Escudo de la privacidad sea, en esencia, equivalente a la de la UE.

ÍNDICE

1. INTRODUCCIÓN

A raíz de la sentencia dictada por el Tribunal de Justicia de la Unión Europea (en lo sucesivo, el TJUE) el 6 de octubre de 2015 en el asunto Schrems[1], el Grupo de trabajo sobre protección de datos del artículo 29 (en lo sucesivo, el Grupo de trabajo del artículo 29) hizo un llamamiento a los Estados miembros de la Unión Europea (en lo sucesivo, la UE) y las demás instituciones europeas para que entablasen un debate con las autoridades de los Estados Unidos (en lo sucesivo, los EE. UU.) a fin de encontrar soluciones políticas, jurídicas y técnicas que permitan realizar transferencias de datos al territorio de los EE. UU. que respeten los derechos fundamentales.

El 2 de febrero de 2016, tras más de dos años de negociaciones, la Comisión Europea y el Departamento de Comercio de los EE. UU. (DoC, por sus siglas en inglés) alcanzaron un acuerdo político sobre un nuevo marco para los intercambios transatlánticos de datos personales con fines comerciales: el Escudo de la privacidad UE-EE. UU. (en lo sucesivo, el Escudo de la privacidad), con el que se pretende sustituir el antiguo régimen de puerto seguro de los EE. UU.

El 29 de febrero de 2016, la Comisión publicó una Comunicación[2], un proyecto de Decisión de adecuación con textos anexos, que constituirán el Escudo de la privacidad. De conformidad con el artículo 30, apartado 1, letra c), de la Directiva 95/46/CE (en lo sucesivo, la Directiva), el Grupo de trabajo del artículo 29 ha evaluado estos documentos a fin de emitir un dictamen sobre el proyecto de Decisión de adecuación elaborado por la Comisión, incluidos los documentos en que se basa el Escudo de la privacidad. En su evaluación, el Grupo de trabajo del artículo 29 ha dividido la labor entre la evaluación de la parte comercial del Escudo de la privacidad y un análisis de las salvaguardias existentes por lo que se refiere a las excepciones a los principios del Escudo de la privacidad para proteger la seguridad nacional, la actuación policial y el interés público.

A raíz de la sentencia Schrems, el Grupo de trabajo del artículo 29 ha celebrado varias reuniones con delegaciones de la administración de los EE. UU., representantes de organizaciones de la sociedad civil tanto de la UE como de los EE. UU. y académicos, con el fin de preparar la evaluación de las consecuencias de la sentencia Schrems. Durante la evaluación del Escudo de la privacidad, se han seguido celebrando reuniones con la Comisión Europea y representantes de la administración de los EE. UU. En dichas reuniones se han presentado algunas aclaraciones, que también se han tenido en cuenta en el presente dictamen. El Grupo de trabajo del artículo 29 destaca que, en esta fase, tales aclaraciones han sido informales y no se puede considerar que formen parte integrante del proyecto de Decisión de adecuación, ya que todavía no se han formulado por escrito.

Sin embargo, el Grupo de trabajo del artículo 29 acoge con especial satisfacción el compromiso adquirido por el DoC durante estas reuniones de cooperar con las autoridades de

[1] Asunto C-362/14, Maximilian Schrems contra Data Protection Commissioner, 6 de octubre de 2015 (en lo sucesivo, Schrems).
[2] COM(2016)117 final de 29 de febrero de 2016.

protección de datos de los Estados miembros de la UE en lo que respecta a la aplicación del Escudo de la privacidad y prever instrucciones y una interpretación jurídica en relación con la aplicación del Escudo de la privacidad que se publicará en sus páginas web.

1.1 Observaciones generales

1.1.1 Alcance de la evaluación del Grupo de trabajo del artículo 29

En primer lugar, el Grupo de trabajo del artículo 29 tuvo en cuenta el marco de protección de datos aplicable en los Estados miembros de la Unión Europea, incluido el artículo 8 del Convenio Europeo de Derechos Humanos (en lo sucesivo, el CEDH), que protege el derecho a la vida privada y familiar, así como los artículos 7, 8 y 47 de la Carta de los derechos fundamentales de la Unión Europea (en lo sucesivo, la Carta), que protegen respectivamente el derecho a la vida privada y familiar, el derecho a la protección de los datos personales y el derecho a la tutela judicial efectiva y a un juicio justo. También tuvo en cuenta la jurisprudencia pertinente y los requisitos de la Directiva.

El requisito de que los terceros países garanticen un nivel de protección de datos adecuado quedó mejor definido por el TJUE en Schrems. El Tribunal de Justicia no solo explicó que las disposiciones de la Directiva deben interpretarse «a la luz de los derechos fundamentales protegidos por la Carta»[3], y en particular por sus artículos 7 y 8, sino que también indicó que el concepto de «nivel de protección adecuado» debe entenderse en el sentido de que «exige que ese tercer país garantice efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en la Unión por la Directiva 95/46, entendida a la luz de la Carta»[4]. En el caso de la antigua Decisión de puerto seguro, tal valoración no se ha realizado nunca con un nivel de detalle suficiente. El Grupo de trabajo del artículo 29 consideró por tanto el proyecto de Decisión de adecuación a la luz del requisito de proporcionar un análisis del nivel de protección de los derechos y libertades fundamentales *sustancialmente equivalente* al garantizado en la UE. El Grupo de trabajo del artículo 29 destaca que el presente dictamen recoge sus principales preocupaciones, pero que, habida cuenta del escaso tiempo transcurrido desde que se publicó el proyecto de Decisión de adecuación, más adelante podrían apreciarse otras cuestiones.

El Grupo de trabajo del artículo 29 constata que, al definir el término «adecuado» en el artículo 25, apartado 6, de la Directiva como «sustancialmente equivalente», el TJUE detalla en mayor medida la adecuación en el asunto Schrems. El Tribunal ha destacado que, aunque el concepto de «nivel de protección adecuado» no exige que el tercer país garantice un nivel de protección idéntico al garantizado en el ordenamiento jurídico de la UE, debe entenderse en el sentido de que exige que ese tercer país garantice efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en la Unión por la Directiva 95/46, entendida a la luz de la Carta.

[3] Schrems, apartado 38.
[4] Schrems, apartado 73.

1.1.2 Evaluación de la parte comercial del proyecto de Decisión de adecuación

El Grupo de trabajo del artículo 29 ya ha explicado en su documento de trabajo 12, «Transferencias de datos personales a terceros países: Aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE»[5], la manera en que ha aplicado los principios básicos de la protección de datos de la UE a las transferencias de datos personales a terceros países. El Grupo de trabajo del artículo 29 intentó encontrar garantías equivalentes que garantizasen un nivel equivalente de protección de los principios garantizados en la Directiva, en especial por lo que respecta a la limitación de la finalidad, la calidad y la proporcionalidad de los datos, la transparencia, la seguridad, los derechos de acceso, rectificación y oposición, la conservación de los datos y las restricciones de las transferencias posteriores. En los dictámenes emitidos por el Grupo de trabajo del artículo 29 en el momento de la valoración inicial de la Decisión de adecuación del puerto seguro[6], así como en las recomendaciones formuladas por el Grupo de trabajo en su carta a la anterior Vicepresidenta y Comisaria de Justicia de la UE Viviane Reding, publicada el 10 de abril de 2014, se aplicó un método similar[7].

1.1.3 Evaluación de las excepciones para el acceso por parte de las autoridades públicas y sus salvaguardias

La evaluación de las excepciones para el acceso de las autoridades públicas a los datos personales cubiertos por el Escudo de la privacidad es compleja, especialmente teniendo en cuenta la sensibilización cada vez mayor de las autoridades de protección de datos y del público en general ante los programas de vigilancia de los EE. UU., a raíz las revelaciones de Snowden. El Grupo reconoce y acoge con satisfacción los esfuerzos realizados por el Gobierno de los EE. UU. a fin de aumentar la transparencia de los programas de vigilancia y su voluntad de incluir salvaguardias adicionales en el Escudo de la privacidad. Al mismo tiempo, el Grupo de trabajo del artículo 29 destaca que cualquier injerencia en los derechos fundamentales a la vida privada y a la protección de datos debe ser justificable en una sociedad democrática. El Tribunal de Justicia criticó el hecho de que la Decisión de puerto seguro no contuviera ninguna apreciación en cuanto a la existencia, en los EE. UU., de normas adoptadas por el Estado para limitar las injerencias. Tampoco se refiere a la existencia de una protección jurídica efectiva contra injerencias de este tipo[8].

Por consiguiente, el Grupo de trabajo del artículo 29 ha analizado el marco jurídico vigente y las prácticas actuales de las agencias de inteligencia de los EE. UU. tal como se detallan en los anexos del proyecto de Decisión, así como las condiciones en que se permite la existencia de injerencias en los derechos fundamentales al respeto de la vida privada y la protección de datos bajo el marco jurídico europeo.

[5] Documento de trabajo aprobado por el Grupo de trabajo el 24 de julio de 1998. Véase en particular su página 6.
[6] Véase WP62, WP32, WP27, WP23, WP21, WP19, WP15 y WP7.
[7] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf .
[8] Schrems, apartados 87 y 88.

Para valorar si una injerencia sería justificable en una sociedad democrática, la evaluación se llevó a cabo a la luz de la jurisprudencia europea sobre los derechos fundamentales, que establece cuatro garantías esenciales[9] relativas a las actividades de inteligencia:

A. El tratamiento debe ser conforme a la ley y basarse en normas claras, precisas y accesibles: esto significa que cualquier persona razonablemente informada debe ser capaz de prever lo que puede ocurrir con sus datos cuando se transfieren;
B. Se han de demostrar la necesidad y la proporcionalidad en relación con los objetivos legítimos perseguidos: se ha de encontrar un equilibrio entre el objetivo para el que se recopilan los datos y se accede a los mismos y los derechos de la persona;
C. Debería existir un mecanismo de supervisión independiente, que sea a la vez eficaz e imparcial: este puede ser un juez u otro órgano independiente, siempre que tenga capacidad suficiente para llevar a cabo los controles necesarios;
D. Debe haber una tutela judicial efectiva disponible para el interesado: cualquier persona debe tener derecho a defender sus derechos ante un organismo independiente.

1.2 Proyecto de Decisión de adecuación

En primer lugar, el Grupo de trabajo del artículo 29 acoge con satisfacción que se pueda poner en marcha un nuevo procedimiento de adecuación en un plazo inferior a seis meses desde que el Tribunal de Justicia declarase inválida la Decisión de puerto seguro. Dada la cantidad de transferencias diarias de datos entre la UE y los EE. UU., que el Grupo de trabajo del artículo 29 reconoce como una parte vital de la economía a ambos lados del Atlántico, se necesita certeza jurídica lo antes posible.

Sin embargo, el Grupo de trabajo del artículo 29 lamenta que el proyecto de Decisión de adecuación publicado por la Comisión no incluya una evaluación exhaustiva de la legislación nacional y los compromisos internacionales de los EE. UU. en forma de informe de adecuación, como ha sido práctica habitual en el pasado en procedimientos similares y en consonancia con el artículo 25 de la Directiva. Esto ha impedido al Grupo de trabajo del artículo 29 realizar un análisis completo del contexto jurídico en el que operará el Escudo de la privacidad. El Grupo de trabajo observa, por ejemplo, que el actual proyecto de Decisión de adecuación no incluye conclusiones sobre la legislación relativa a privacidad y protección de datos en los EE. UU., ni a nivel federal ni a nivel estatal, incluida la legislación sectorial, ni sobre la legislación que permite formas de acceso público relacionadas con la no vigilancia. Tampoco se ha definido la relación entre las transferencias de datos con arreglo al Escudo de la privacidad y a otros resultados de adecuación existentes, como el Acuerdo entre la UE y EE. UU. sobre el registro de nombres de los pasajeros (PNR, por sus siglas en inglés) y el Acuerdo sobre el Programa de Seguimiento de la Financiación del Terrorismo (TFTP, por sus siglas en inglés).

[9] Las garantías esenciales europeas se basan en la jurisprudencia del TJUE y del TEDH y se exponen con más detalle en el documento de trabajo del Grupo de trabajo del artículo 29 WP237, publicado el 13 de abril de 2016.

1.2.1 Ámbito de aplicación del marco de protección de datos de la UE y, en particular, de los principios de la Directiva 95/46/CE

El Grupo de trabajo del artículo 29 recuerda que, con arreglo al marco jurídico de la UE sobre protección de datos y, en particular, de conformidad con la Directiva (artículo 4, apartado 1), las normas jurídicas de los Estados miembros no solo se aplican a las operaciones de tratamiento realizadas por responsables del tratamiento establecidos en su territorio, sino también cuando los responsables del tratamiento (aunque no estén establecidos en la UE) hagan uso de equipos situados en el territorio de la UE, en particular, para la recopilación de datos personales. En consecuencia, la legislación de los Estados miembros de la UE se aplica a cualquier tratamiento que tenga lugar con anterioridad a la transferencia a los EE. UU., ya sea en el contexto de actividades de entidades establecidas en la UE o mediante el uso de equipos situados en la UE utilizados por entidades no establecidas en la UE. El Grupo de trabajo del artículo 29 pide que ello se indique explícitamente en el proyecto de Decisión de adecuación.

Debe quedar claro que los principios del Escudo de la privacidad se aplicarán desde el momento en que tenga lugar la transferencia. Además, el Grupo de trabajo del artículo 29 recuerda que los responsables de tratamiento de datos establecidos en la UE que transfieran datos a un encargado del tratamiento de datos en los EE. UU. siguen estando sujetos a la normativa de protección de datos de la UE.

1.2.2 Falta de claridad de los documentos del Escudo de la privacidad

El hecho de que los principios y las garantías concedidas por el Escudo de la privacidad figuren tanto en la Decisión de adecuación como en sus anexos hace que la información resulte difícil de encontrar y, a veces, sea incoherente. Esto contribuye a una falta general de claridad acerca del nuevo marco y a dificultar aún más la accesibilidad para los interesados, las entidades y las autoridades de protección de datos. Por otra parte, el texto adolece de falta de claridad lingüística. Por consiguiente, el Grupo de trabajo del artículo 29 insta a la Comisión a proponer conceptos que resulten claros y comprensibles a ambos lados del Atlántico.

El Grupo de trabajo del artículo 29 propone incluir un anexo en el que se definan las condiciones básicas que se aplican en los documentos del Escudo de la privacidad. Para el buen funcionamiento del Escudo de la privacidad a ambos lados del Atlántico es esencial que exista una forma común y sin ambigüedades de entender las obligaciones impuestas por la Decisión de adecuación, por lo que al Grupo de trabajo del artículo 29 le preocupa que, debido a la abundancia de referencias cruzadas y formulaciones no normalizadas, así como a la complejidad de los documentos, surjan dificultades en relación con la coherencia, la inteligibilidad y la claridad de la aplicación del Escudo.

Y lo que es más importante: en los documentos del Escudo de la privacidad se hace uso de terminología que no es coherente con la que se suele utilizar en la UE en materia de protección de datos. Ello no representa necesariamente un problema, en la medida en que esté

claro cuál sería la terminología correspondiente con arreglo al Derecho de la UE (y cuál con arreglo a la legislación de los EE. UU.). No obstante, el Grupo de trabajo del artículo 29 lamenta observar que este no es el caso, ni siquiera en el propio proyecto de Decisión de adecuación. Por ejemplo, la palabra «acceso» se utiliza en el capítulo 3 del proyecto de Decisión de adecuación en un sentido que implica la recopilación de datos personales, y no en el sentido de permitir a alguien que vea los datos ya recogidos. El acceso de las empresas a los datos y el derecho de acceso de los particulares son dos conceptos distintos que no deben confundirse.

El Grupo de trabajo del artículo 29 destaca que la terminología debe emplearse también de forma coherente en todos los documentos dados, incluido el proyecto de Decisión de adecuación. Este no es el caso actualmente, por ejemplo, con los conceptos de «tratamiento» y «datos personales». Ambos están, en principio, bien definidos en el anexo II, pero no se aplican de forma coherente en todo un documento, lo que da lugar a lagunas en la protección[10,11].

El Grupo de trabajo del artículo 29 acoge con satisfacción que en los documentos constitutivos del Escudo de la privacidad se hayan incluido las definiciones de algunos de los términos empleados. Sin embargo, esto no se ha hecho en el caso de algunos otros términos fundamentales, como «agente» o «encargado del tratamiento», «datos codificados», «datos anónimos» y «particular de la UE», que en opinión del Grupo de trabajo del artículo 29 merecen una definición clara y consensuada entre los EE. UU. y la UE a fin de evitar confusiones en una fase posterior, tanto para los responsables y encargados del tratamiento de datos que utilicen el Escudo de la privacidad, como para las autoridades de control y el público en general. Una solución fácil sería integrar un glosario en las preguntas frecuentes del Escudo de la privacidad.

El Grupo de trabajo del artículo 29 señala asimismo los motivos legítimos para el tratamiento de datos sensibles en el principio complementario 1 (anexo II, Sec. III.1.), en los casos en que una entidad no tiene que obtener el consentimiento expreso (aceptación). Puede entenderse que este principio complementario 1 detalla los motivos legítimos de la recogida de datos en

[10] Algunas de las cláusulas únicamente enumeran ciertos tipos de operaciones de tratamiento de datos, en lugar de utilizar el término «tratamiento». Esto da lugar a vacíos en la protección. Por ejemplo, según el texto del anexo II, Sec. III.6.f., los principios del Escudo de la privacidad solo serían aplicables cuando la entidad «almacene, utilice o divulgue» los datos recibidos (es decir, no para las demás operaciones cubiertas por el término «tratamiento», tales como la recogida, la grabación, la modificación, la recuperación, la consulta y la supresión). La seguridad de los datos se impondría únicamente para crear, mantener, utilizar o difundir información personal (anexo II, Sec. II.4.). La definición de los datos personales también se limita a los datos «recibidos» y «registrados». Otro ejemplo: el principio de notificación (anexo II, Sec.II.1a. iv.) afirma que la entidad certificada deberá informar a los interesados de «los fines para los que recogen y utilizan información sobre ellos». En el anexo II, Sec. III.9.a.11. únicamente se mencionan los datos que se transfieren o a los que se accede. Aunque parece que en la mayor parte de estos casos no se pretende limitar el alcance de los principios ni crear lagunas de protección, este cambio de terminología conlleva un riesgo de lagunas. Dado que el término «tratamiento» se define en los principios, es fundamental hacer uso de él de manera coherente, a fin de evitar los vacíos existentes en la actualidad. En caso contrario habría demasiado margen para interpretaciones presumiblemente no deseadas que podrían dar lugar a una interpretación inadecuada de los términos de la Decisión.

[11] La definición de «datos personales» que figura en el anexo II, Sec. I.8.a., se refiere a «datos referidos a una persona identificada o identificable». No obstante, el principio complementario establece que, en relación con los datos sobre recursos humanos, los principios solo se aplican cuando se transfieren registros identificados o se accede a ellos. El Grupo de trabajo del artículo 29 considera que esto abre la posibilidad de tratar los datos personales de una manera que no es conforme con los principios de protección de datos en virtud del Derecho de la UE ni con la definición general de datos personales de conformidad con el Escudo de la privacidad.

la UE, pues la lista es similar al artículo 8 de la Directiva. El Grupo de trabajo del artículo 29 desea recordar que cualquier tratamiento (incluidas la recogida y la transferencia) de datos sensibles sujetos a legislación de la UE ha de responder a razones legítimas con arreglo al artículo 8 de la Directiva. No se puede interpretar que el Escudo de la privacidad ofrezca criterios alternativos para tal tratamiento de datos. Por ejemplo, en opinión del Grupo de trabajo del artículo 29 no es posible que una entidad estadounidense recoja datos sujetos a la legislación de la UE sobre la base de la legislación laboral estadounidense (véase el anexo II, Sec. III.1.a.v.). El Grupo de trabajo del artículo 29 señala, por lo tanto, que cualquier interpretación del principio complementario 1 solo puede conducir a su aplicación a datos sensibles ya transferidos después de haber sido recogidos en la UE por motivos legítimos enumerados en el artículo 8 de la Directiva.

El Grupo de trabajo del artículo 29 señala por último la falta de claridad en cuanto a la cuestión de quién puede considerarse un particular de la UE y, por tanto, beneficiarse de la protección del Escudo de la privacidad: todos los ciudadanos de la UE o todas las personas que residen en la UE. Esto reviste especial importancia en relación con el derecho al recurso, incluido el acceso al mecanismo del Defensor del Pueblo. Además, la Decisión de adecuación debería abordar la cuestión de en qué medida el Escudo de la privacidad se aplicará también a los ciudadanos y residentes de los países del EEE y Suiza, que en el pasado estaban cubiertos por el régimen de puerto seguro.

1.2.3 Revisión conjunta y suspensión

El Grupo de trabajo del artículo 29 acoge con satisfacción que la Comisión Europea y el Gobierno de los EE. UU. hayan convenido en revisar periódicamente la aplicación práctica del Escudo de la privacidad. Esta revisión conjunta se realiza en la comunidad de protección de datos de la UE desde hace varios años, especialmente en relación con los acuerdos sobre el intercambio de datos PNR con terceros países y el acuerdo TFTP. El Grupo de trabajo del artículo 29 acoge además con satisfacción que un número indeterminado de representantes de las autoridades de protección de datos pueda participar en estas revisiones conjuntas.

Dada la experiencia en revisiones conjuntas que ha adquirido en los últimos años, el Grupo de trabajo del artículo 29 desea dejar claro que espera que la revisión conjunta del Escudo de la privacidad sea más amplia que las revisiones conjuntas del PNR y el TFTP. En particular, es conveniente que la revisión conjunta no incluya únicamente reuniones con representantes de organismos, entidades y empresas de los EE. UU., sino también verificaciones sobre el terreno de ciertos elementos del Escudo de la privacidad. Los representantes de la autoridad de protección de datos (en lo sucesivo, APD) en el examen conjunto han de poder hacer sugerencias de cara a estas verificaciones sobre el terreno.

El Grupo de trabajo del artículo 29 considera que una revisión conjunta requiere una evaluación conjunta de los resultados. Hasta la fecha, los resultados de las revisiones conjuntas se han presentado en un documento de los servicios de la Comisión para el que no era necesaria la aprobación de los miembros del equipo de revisión conjunta externos a la Comisión. En la revisión conjunta del Escudo de la privacidad, el Grupo de trabajo del

artículo 29 valoraría positivamente que el informe de los resultados pudiera ser un producto compartido. Alternativamente, cabría considerar la posibilidad de que una APD independiente realizase otro informe de revisión conjunta.

Por último, en lo referente a la revisión conjunta, el Grupo de trabajo del artículo 29 recuerda la promesa de la Comisión de que los gastos efectuados por los representantes del Grupo de trabajo del artículo 29 durante las revisiones conjuntas serán reembolsados por la Comisión. El Grupo asume que lo dicho también es aplicable a la revisión conjunta del Escudo de la privacidad, en cualquier caso para un número razonable de representantes de la autoridad de protección de datos.

El Grupo de trabajo del artículo 29 recomienda que, a más tardar tres meses antes de la primera revisión conjunta del Escudo de la privacidad, la Comisión, el Gobierno de EE. UU. y el Grupo de trabajo del artículo 29 acuerden las modalidades de revisión conjunta y las recojan por escrito.

1.2.4 Marco jurídico de la UE en curso de revisión

La Decisión de adecuación del Escudo de la privacidad es la primera Decisión de adecuación redactada tras el acuerdo de principio sobre el texto del Reglamento general de protección de datos. Sin embargo, el Grupo de trabajo del artículo 29 ha observado que el Escudo de la privacidad no refleja aún la situación futura. Por ejemplo, en el Escudo de la privacidad no se han incluido nuevos conceptos importantes tales como el derecho a la portabilidad de los datos y las obligaciones adicionales de los supervisores de datos, incluida la necesidad de llevar a cabo evaluaciones de impacto de la protección de datos y de cumplir los principios de la privacidad desde el diseño y la privacidad por defecto. Por lo tanto, el Grupo de trabajo del artículo 29 desea sugerir que el Escudo de la privacidad, como cualquier posible decisión de adecuación, se revise poco tiempo después de la entrada en vigor del Reglamento general de protección de datos. Se agradecería una referencia explícita a este proceso de revisión de la Decisión de adecuación final.

2. EVALUACIÓN DE LA PARTE COMERCIAL DEL PROYECTO DE DECISIÓN DE ADECUACIÓN

2.1 Observaciones generales

2.1.1 Mejoras

El Grupo de trabajo del artículo 29 acoge con satisfacción las mejoras introducidas por el Escudo de la privacidad y la voluntad de sus negociadores de intentar abordar las carencias del puerto seguro que había señalado. En particular, en comparación con el régimen de puerto seguro, se pueden observar mejoras en los siguientes elementos: la introducción de algunas definiciones clave, como «datos personales», «tratamiento» y «responsable del tratamiento», los mecanismos establecidos para garantizar la supervisión de la lista del Escudo de la privacidad, y las revisiones internas o externas de conformidad, que ahora son obligatorias. También se han aplicado mejoras al principio de acceso y el Grupo de trabajo del artículo 29

señala que ahora se prevén los derechos de rectificación y supresión cuando los datos se utilizan de forma incompatible con los principios del Escudo de la privacidad. Además, ahora queda claro que los particulares deben recibir tanto la confirmación de que se están tratando datos que les conciernen como la comunicación de los datos tratados.

El Grupo de trabajo del artículo 29 acoge asimismo con satisfacción el refuerzo de las garantías jurídicas cuando se están llevando a cabo transferencias ulteriores y los compromisos del DoC y la Comisión Federal de Comercio para hacer cumplir las obligaciones establecidas por el Escudo de la privacidad.

2.1.2 Aplicación del Escudo de la privacidad a entidades que actúen como encargados del tratamiento (agente)

Lamentablemente, sigue sin estar claro en qué medida los principios del Escudo de la privacidad son aplicables a las entidades certificadas que reciben de la UE datos personales con fines de mera transformación (denominados «agentes» o «encargados del tratamiento»). Si bien las disposiciones del anexo II, Sec. III.10.a., mencionan las transferencias de datos a las entidades certificadas para estos fines (al hacer referencia a la necesidad de celebrar un contrato), carecen de indicaciones sobre cómo aplicar el Escudo de la privacidad a los encargados del tratamiento (agentes). Ello genera incertidumbre tanto entre las entidades certificadas de los EE. UU. que reciben datos con fines de tratamiento como entre las empresas de la UE que llevan a cabo transferencias de datos a entidades certificadas que actúan como encargados del tratamiento, así como entre las personas cuyos datos son objeto de tratamiento. En consecuencia, será difícil determinar qué obligaciones son efectivamente aplicables a las organizaciones del Escudo que realizan el tratamiento de datos personales recibidos de la UE en su papel de encargados del tratamiento. Así pues, no cabe duda de que se precisa una aclaración.

Se ha de tener en cuenta que varias de las obligaciones incluidas en los principios no son adecuadas para los encargados del tratamiento, pues es siempre el responsable del tratamiento de datos el que determina los fines y medios de este (véase la definición de «responsable del tratamiento de datos» en el anexo II, Sec. I.8.c.). Es por esta razón por la que algunas de las obligaciones contenidas en los principios pueden, en el caso de que se apliquen a una entidad que actúe en calidad de agente, ser contrarias al contrato de tratamiento de datos exigido por la legislación de la UE (el contrato mencionado en el anexo II, Sec. III.10.a.). Por ejemplo, en general el contrato de tratamiento de datos no autorizará al encargado del tratamiento de datos (agente) a la transferencia ulterior de datos a un tercero responsable del tratamiento, ni siquiera en las circunstancias mencionadas en el anexo II, Sec. II.3.a.). Las transferencias ulteriores a terceros agentes solo se deben autorizar tras la aprobación del responsable del tratamiento de datos. Además, de acuerdo con los requisitos de la legislación de la UE, el encargado del tratamiento (agente) no podrá proporcionar a los particulares la notificación completa de acuerdo con lo previsto por el principio de notificación (anexo II, Sec. II.1.), por ejemplo porque la entidad no determina los fines del tratamiento.

Es esencial, por lo tanto, precisar en los principios que, en caso de contradicción, prevalecerán las disposiciones del contrato de tratamiento de datos y, en particular, las instrucciones de la entidad que transfiere los datos fuera de la UE. Sin esta aclaración, los principios podrían interpretarse y aplicarse de una forma que confiera demasiadas capacidades de control al agente del Escudo de la privacidad, lo que conllevaría un riesgo de que el exportador de datos de la UE vulnerara sus obligaciones como responsable del tratamiento de datos en virtud de la normativa europea de protección de datos a la que está sujeto a la hora de transferir datos a una organización del Escudo que actúe como agente. Además, esta falta de claridad da la impresión de que el transformador puede reutilizar los datos como desee.

Asimismo, deben fijarse normas específicas para cuando una entidad actúe como encargado del tratamiento de datos (agente), a fin de garantizar que esa entidad respete las instrucciones del responsable del tratamiento. Debe quedar claro que las entidades de los EE. UU. que reciban datos con fines de mera transformación no pueden tratar los datos por cuenta propia. En ausencia de normas específicas aplicables a las entidades que actúan como encargados del tratamiento, es difícil determinar con arreglo a qué normas puede autocertificarse el encargado del tratamiento (agente).

2.1.3 Limitaciones a la obligación de observación de los principios

El anexo II, Sec. I.5., dispone, entre otras cosas, exenciones a los principios cuando los datos cubiertos por el Escudo de la privacidad se utilicen por exigencias de seguridad nacional[12], interés público o cumplimiento de la ley, o bien por disposición legal o reglamentaria, o jurisprudencia que origine conflictos de obligaciones o prevea autorizaciones explícitas. Sin un conocimiento exhaustivo de la legislación de los EE. UU., tanto a nivel federal como a nivel estatal, es difícil para el Grupo de trabajo del artículo 29 evaluar el ámbito de aplicación de esta exención y examinar si dichas limitaciones son justificables en una sociedad democrática. Es esencial que la Comisión Europea también incluya en su proyecto de Decisión de adecuación un análisis del nivel de protección en los casos en que se aplicarían dichas exenciones. El Grupo de trabajo del artículo 29 insta a la Comisión a que garantice que la UE está informada de cualquier acto legislativo o normativa gubernamental que afecte a la observancia de los principios aplicables actualmente o en el momento en que los nuevos estatutos o reglamentos entren en vigor en los EE. UU.

2.1.4 Falta de un principio de limitación de la conservación de datos

El principio de limitación de la conservación de datos [artículo 6, apartado 1, letra e) de la Directiva] es un principio fundamental de la normativa europea de protección de datos por el que se establece que los datos personales solo deben conservarse durante el tiempo necesario para alcanzar los fines para los que fueron recogidos o para los que se traten ulteriormente.

Sin embargo, el Grupo de trabajo del artículo 29 no puede encontrar en los documentos constitutivos del Escudo de la privacidad ninguna referencia a la necesidad de que los

[12] Véanse en el capítulo 3 más comentarios sobre el uso de los datos personales cubiertos por el Escudo de la privacidad con fines de seguridad nacional y, en el capítulo 4, con fines policiales.

responsables del tratamiento de datos velen por que los datos se eliminen una vez que el fin para el que fueron recogidos o tratados ulteriormente haya quedado obsoleto. Por lo tanto, según parece, los principios no imponen a las entidades certificadas un límite para el período de retención de datos comparable al que viene impuesto por el principio de limitación de la conservación de datos en virtud del Derecho de la UE.

No puede considerarse en modo alguno que el texto del principio de integridad de los datos y de limitación de la finalidad (anexo II, Sec. II.5.) obligue a las entidades que actúan como responsables del tratamiento a suprimir los datos una vez que ya no sean necesarios para los fines para los que hayan sido recogidos o sometidos a un tratamiento ulterior, ni a las entidades que actúan como encargados del tratamiento a suprimir los datos una vez expirado el acuerdo de servicios.

El Grupo de Trabajo subraya que la falta de disposiciones que impongan un límite a la conservación de datos en virtud del Escudo de la privacidad brinda a las entidades la posibilidad de conservar los datos mientras lo deseen, incluso después de desvincularse del Escudo de la privacidad, lo cual no es conforme con el principio esencial de limitación de la conservación de datos.

2.1.5 Falta de garantías en las decisiones automatizadas que tiene efectos jurídicos o afecta de manera significativa a los particulares

El Escudo de la privacidad no ofrece ninguna garantía jurídica cuando las personas se ven sometidas a una decisión con efectos jurídicos que les concierne o afecta de manera significativa y que se basa únicamente en un tratamiento automatizado de datos destinado a evaluar cuestiones personales como el rendimiento laboral, el crédito, la fiabilidad, la conducta, etc.

El Grupo de trabajo del artículo 29 ya ha destacado en su documento de trabajo 12 la necesidad de prever garantías jurídicas para las decisiones automatizadas (que produzcan efectos jurídicos o afecten de manera significativa al individuo) con el fin de proporcionar un nivel de protección adecuado.

Esta necesidad se hace incluso más vital porque las nuevas tecnologías en continuo desarrollo permiten a más empresas plantearse la posibilidad de aplicar mecanismos automatizados de toma de decisiones que pueden debilitar la posición de las personas, que se ven despojadas de todo recurso contra dichas decisiones, tomadas por ordenador. En los casos en que las decisiones adoptadas únicamente por sistemas automatizados repercuten en la situación jurídica de los interesados o les afectan de manera significativa (por ejemplo, mediante su inclusión en listas negras, lo que priva a los particulares de sus derechos) es fundamental ofrecer garantías suficientes que incluyan el derecho a conocer la lógica aplicada y a solicitar un nuevo examen de carácter no automatizado.

2.1.6 Período transitorio para las relaciones comerciales existentes

El Escudo de la privacidad prevé la aplicación inmediata de los principios tras la certificación. No obstante, las entidades certificadas en los dos primeros meses siguientes a la fecha efectiva de entrada en vigor del Escudo de la privacidad tendrán que adecuar lo antes posible toda relación comercial existente con terceros al principio de responsabilidad de la transferencia ulterior. En cualquier caso, deben hacerlo en un plazo máximo de nueve meses a partir de la certificación de adhesión al Escudo de la privacidad.

Esto significa que los contratos existentes han de ponerse, en la medida necesaria, en consonancia con los principios entre dos y nueve meses después de la certificación. Durante este período transitorio, basta con aplicar los principios de notificación y opción. El Grupo de trabajo del artículo 29 hace hincapié en el hecho de que se puedan llevar a cabo transferencias sobre la base del Escudo de la privacidad solo a partir del momento en que la entidad pueda cumplir plenamente todos los requisitos del Escudo. No se puede considerar que la posibilidad de enviar datos durante un período transitorio sin que el destinatario esté en condiciones de cumplir plenamente los principios del Escudo satisfaga las condiciones de una transferencia legal y, por tanto, no es aceptable.

2.2 Observaciones específicas

2.2.1 Transparencia

a) Observaciones generales sobre la notificación

El Grupo de trabajo del artículo 29 acoge con satisfacción los requisitos más completos y detallados establecidos en virtud del principio de notificación, en particular que la notificación deba incluir un vínculo o una dirección web del Escudo de la privacidad y se refiera al derecho de acceso de las personas, así como a los mecanismos alternativos de resolución de conflictos.[13] Sin embargo, el Grupo de trabajo del artículo 29 propone ser más explícito en relación con los otros derechos cubiertos (a corregir o suprimir cuando los datos sean inexactos o hayan sido tratados incumpliendo los principios).

Los documentos constitutivos del Escudo de la privacidad suscitan preocupación en relación con el momento en el que una organización del Escudo de la privacidad ha de hacer una notificación a un particular. El anexo II, Sec. II.1.b., establece que «la notificación se hará [...] la primera vez que se invite a los particulares a proporcionar a la entidad información personal o, posteriormente, tan pronto como sea posible, pero en cualquier caso antes de que la entidad use dicha información para un fin distinto de aquel con el que inicialmente la recogió o trató la entidad que la transfiere o la divulga por primera vez a un tercero». El Grupo de trabajo del artículo 29 considera que, en muchos casos, una organización del Escudo de los EE. UU. no recogerá directamente los datos del interesado, por lo que la

[13] Anexo II, Sec.II.1. El Grupo de trabajo del artículo 29 hace referencia igualmente a la segunda recomendación de la Comisión formulada en la Comunicación COM(2103)847, así como en la carta del Grupo de trabajo del artículo 29 a la Vicepresidenta Reding de 10 de abril de 2014, y en particular el punto 4 del epígrafe «Transparencia».

notificación se debe hacer en el momento en el que la organización del Escudo registre los datos.

El Grupo de trabajo del artículo 29 señala que la aplicación efectiva de los requisitos en lo que respecta al principio de notificación y la política de privacidad debe evaluarse en la primera revisión anual del Escudo de la privacidad.

b) Disponibilidad pública de la política de privacidad

El Grupo de trabajo del artículo 29 acoge con satisfacción que se haya expresado de manera explícita que el DoC comprobará si las empresas que disponen de sitios web públicos han publicado su política de privacidad en esos sitios web o, si no tienen sitios web públicos, dónde se pone la política de privacidad a disposición del público[14].

c) Publicación de las condiciones de privacidad de los contratos con los encargados del tratamiento

El Escudo de la privacidad prevé, entre las condiciones con arreglo a las cuales las organizaciones del Escudo de la privacidad pueden transferir datos a un encargado del tratamiento (agente), la obligación de que las entidades autocertificadas proporcionen «un resumen o una copia representativa de las correspondientes disposiciones de privacidad de su contrato con ese agente» (anexo II, Sec. II.3.b.v.). El Grupo acoge con satisfacción este requisito de transparencia respecto del DoC.

2.2.2 Opción

El Escudo de la privacidad prevé un derecho de exclusión voluntaria de la divulgación de datos personales a un tercero o a la utilización de datos personales para un uso sustancialmente diferente[15] (anexo II, Sec. III.2.). Además, los particulares gozan de un derecho de exclusión voluntaria del uso de información personal con fines de comercialización directa en cualquier momento (anexo II, Sec. III.12.a.)[16].

Excepto en el contexto de los fines directamente comerciales, no se facilitan detalles sobre la manera y el momento en que puede ejercerse esta exclusión voluntaria. El Grupo de trabajo del artículo 29 considera que la simple referencia a la existencia de este derecho en la política de privacidad no puede ser suficiente, y que *antes* de la publicación o la reutilización de información personal se debe brindar una oportunidad *individualizada* de ejercer este derecho.

Además, el Grupo de trabajo del artículo 29 hace hincapié en que en el Escudo de protección de la intimidad deberá ofrecerse un derecho general a oponerse (por razones imperiosas

[14] Véase la primera recomendación formulada por la Comisión Europea en su Comunicación COM(2013)847 y la carta del Grupo de trabajo del artículo 29 a la Vicepresidenta Reding de 10 de abril de 2014, y en particular su punto 3 del epígrafe «Transparencia».
[15] El principio complementario 14.c.i. prevé el derecho a retirarse de un ensayo clínico, que se podría considerar como el derecho a oponerse o a retirar el consentimiento.
[16] Esto es idéntico a lo previsto en el régimen de puerto seguro (pregunta frecuente 12) y no se ha efectuado ningún cambio a este respecto.

relacionadas con la situación particular del interesado), entendiéndose por tal el derecho a pedir que se finalice el tratamiento de los datos propios, siempre que el particular tenga motivos legítimos imperiosos relacionados con esa situación particular[17]. El Grupo de trabajo del artículo 29 recomienda encarecidamente que el proyecto de Decisión de adecuación establezca claramente que debe existir el derecho a oponerse en cualquier momento, y que dicha oposición no se limite al uso de los datos para fines de mercadotecnia directa[18].

El Grupo de trabajo del artículo 29 teme que la falta de definición de lo que ha de considerarse un fin «sustancialmente diferente» dé lugar a confusión e inseguridad jurídica. Debería aclararse que, en todo caso, el principio de opción no puede utilizarse para eludir el principio de limitación de la finalidad[19]. El principio de opción debe aplicarse únicamente si el fin es sustancialmente diferente pero compatible, dado que el tratamiento con fines incompatibles está prohibido (anexo II, Sec. II.5.a.). Debe aclararse que el derecho de exclusión voluntaria no puede permitir a la entidad utilizar los datos para fines incompatibles. Por lo tanto, recomienda armonizar el texto correspondiente mediante un texto único y definido (por ejemplo, «fin sustancialmente diferente pero compatible»).

Convendría aclarar cuándo entra dentro del ámbito de aplicación de la legislación de la UE la decisión de tratar los datos para otros fines o de divulgar información. En esta situación, las condiciones jurídicas habituales de la UE en relación con este tratamiento (como la prohibición de tratamiento con fines incompatibles, el establecimiento de un motivo legítimo para el tratamiento y la necesidad de informar al particular) se aplican también directamente a la entidad de los EE. UU. que entra en el ámbito de aplicación de la legislación de la UE. En la práctica, esto supone que corresponde al exportador de la UE adoptar una decisión de este tipo para garantizar la transparencia y la legitimidad del tratamiento de conformidad con la legislación de la UE. Por lo tanto, el principio de opción únicamente puede aplicarse en el caso de que la decisión la tome exclusivamente la organización del Escudo de los EE. UU. no sometida a la legislación de la UE.

2.2.3 Transferencias ulteriores

a) Ámbito de aplicación

El Grupo de trabajo del artículo 29 está preocupado por las situaciones en la que las transferencias ulteriores de datos personales se efectúan desde una entidad certificada del Escudo de la privacidad de los EE. UU. a un destinatario de un tercer país.

El Escudo no se debe considerar únicamente una herramienta para la transferencia de datos de la UE desde la UE a los EE. UU., sino que también servirá como herramienta para la transferencia de datos desde los EE. UU. a terceros países. Las disposiciones sobre transferencias son, por lo tanto, un elemento importante del Escudo que deberá ofrecer

[18] Véase la carta dirigida por el Grupo de trabajo del artículo 29 a la Vicepresidenta Reding, rúbrica «Opción».
[19] Un ejemplo concreto de tratamiento incompatible adicional autorizado en virtud del principio de opción está previsto en el principio complementario 9.b.i. (véase el comentario del Grupo de trabajo del artículo 29 al respecto, en el punto correspondiente a los «datos sobre recursos humanos).

garantías suficientes y un nivel de protección adecuado cuando se realicen transferencias ulteriores desde fuera de los EE. UU. Un aspecto específico está relacionado con la seguridad nacional y la aplicación de la ley.

El principio de responsabilidad de la transferencia ulterior del Escudo de la privacidad no se limita a los responsables o encargados del tratamiento de datos o agentes establecidos en los EE. UU. Por ello, se pueden efectuar transferencias ulteriores a terceros países sobre la base del Escudo de la privacidad, incluso si el tercer país dispone de legislación que prevea el acceso público a los datos personales, por ejemplo a efectos de vigilancia. Esto sitúa los datos de la UE en situación de riesgo de injerencias injustificadas en la protección de los derechos fundamentales.

En caso de transferencia ulterior a un tercer país, cada organización del Escudo de la privacidad debería estar obligada a evaluar previamente los requisitos obligatorios de la legislación nacional del tercer país aplicable al importador de datos. Si se detecta un riesgo de efecto negativo importante en las garantías, las obligaciones y el nivel de protección ofrecido por el Escudo de la privacidad, la organización del Escudo de la privacidad de los EE. UU. que actúe como encargado del tratamiento (agente) lo notificará de inmediato al responsable del tratamiento de datos de la UE, antes de efectuar cualquier transferencia ulterior. En estos casos, el exportador de datos estará facultado para suspender la transferencia de datos o resolver el contrato. Cuando exista tal riesgo de efecto negativo importante, la organización del Escudo que actúe como responsable no deberá estar autorizada a efectuar transferencias ulteriores de datos, pues ello comprometería su deber de proporcionar el mismo nivel de protección previsto en virtud de los principios en el caso de transferencias ulteriores (véase el anexo II, Sec. II.3.a.).

Asimismo, si en la legislación del país tercero se produce un cambio que probablemente tenga un efecto negativo importante en las garantías, las obligaciones y el nivel de protección ofrecido por el Escudo de la privacidad, la organización del Escudo de la privacidad de los EE. UU. que actúe como encargado del tratamiento (agente) debería estar obligada (por el Escudo de la privacidad) a notificar sin demora al exportador de datos dicho cambio en cuanto tenga conocimiento de él, y en ese caso el exportador estará facultado para suspender la transferencia de datos o resolver el contrato. Por consiguiente, cuando esto suceda, una organización del Escudo que actúe como responsable del tratamiento no deberá estar autorizada a efectuar transferencias ulteriores, pues tiene el deber de ofrecer el mismo nivel de protección que con arreglo a los principios (véase el anexo II, Sec. II.3.a.).

El Grupo de trabajo del artículo 29 recuerda su postura de que, si el responsable del tratamiento de datos de la UE es consciente de una transferencia ulterior a un tercero fuera de los EE. UU. incluso antes que se realice la transferencia a los EE. UU., o si el responsable del tratamiento de datos de la UE es responsable conjuntamente de la decisión de permitir transferencias ulteriores, la transferencia se deberá considerar una transferencia directa de la UE hacia el tercer país fuera de los EE. UU. Esto significa que los artículos 25 y 26 de la Directiva son aplicables a la transferencia en lugar del principio de transferencia ulterior del Escudo de la privacidad.

b) Transferencias desde una organización del Escudo a un tercero responsable del tratamiento

El Grupo de trabajo del artículo 29 acoge con satisfacción la obligación de suscribir un contratos (anexo II, Sec. II.3.a.) que garanticen que el responsable del tratamiento de un tercero proporcione al menos el mismo nivel de protección de la intimidad que se exige en los principios del Escudo de la privacidad. El objetivo es garantizar que los datos personales se sigan protegiendo adecuadamente, incluso después de una transferencia ulterior. Sin embargo, el Grupo de trabajo del artículo 29 formula algunas observaciones sobre las condiciones propuestas.

Falta de referencia al principio de limitación de la finalidad

El Grupo de trabajo del artículo 29 recomienda también la inserción de una referencia clara al principio de limitación de la finalidad (anexo II, Sec. II.5.) conforme a las condiciones de las transferencias ulteriores a un tercero responsable del tratamiento (anexo II, Sec. II.3.a.). De esta forma quedaría claro que no podrán tener lugar transferencias ulteriores cuando el tercero responsable del tratamiento trate los datos para un propósito incompatible.

Exención de la necesidad de suscribir un contrato en caso de transferencias intragrupo entre responsables del tratamiento

En las transferencias intragrupo entre responsables del tratamiento se prevé una exención de la necesidad de suscribir un contrato. En tal situación, los principios establecen que la continuidad de la protección se podría ofrecer mediante normas vinculantes para las empresas u «otros instrumentos intragrupo (por ejemplo, programas de cumplimiento y control)» (anexo II, Sec. III.10.b.). El Grupo de trabajo del artículo 29 considera que la referencia a «otros instrumentos intragrupo» no garantiza los compromisos jurídicamente vinculantes contraídos por los demás miembros del grupo. Dado que el Grupo de trabajo del artículo 29 y la legislación de la UE[20] prefieren en general los compromisos vinculantes de enmarcar las transferencias intragrupo, es importante evitar que el Escudo de la privacidad se utilice para eludir este requisito. El Grupo de trabajo del artículo 29 recuerda que, en cualquier caso, las transferencias ulteriores desde los EE. UU. a terceros países previstas antes incluso de que tenga lugar la transferencia a los EE. UU. o que estén sujetas a una responsabilidad compartida con el responsable del tratamiento de datos de la UE[21] se deben considerar transferencias directas desde la UE a terceros países fuera de los EE. UU. Los artículos 25 y 26 de la Directiva son, por tanto, aplicables a la transferencia.

c) Transferencias desde una organización del Escudo de la privacidad a un tercero encargado (agente)

[20] La necesidad de compromisos vinculantes y ejecutables también se subraya en el Reglamento general de protección de datos independientemente del instrumento utilizado (normas vinculantes para las empresas, cláusulas contractuales, códigos de conducta o certificación).
[21] Por ejemplo, en el caso de los datos sobre recursos humanos.

El Grupo de trabajo del artículo 29 acoge con satisfacción el hecho de que para las entidades destinatarias que actúen como encargados del tratamiento (agentes) sea ahora obligatorio suscribir un contrato de transferencia ulterior independientemente de su participación en el Escudo de la privacidad o de si cuentan con otra solución de constatación de adecuación. El Grupo de trabajo del artículo 29 acoge también con satisfacción las garantías adicionales que se acompañan a estas transferencias ulteriores (anexo II, Sec. II.3.a.i., iii., iv. y v.; y Sec. 7.d.). El último punto (anexo II, Sec. II.7.d.) se refiere a la obligación de responsabilidad cuando los datos se comuniquen a un agente. Sin embargo, parece que esta garantía no se aplicará en caso de que una entidad haya decidido cooperar con una APD (véase el anexo II, Sec. III.5.a., *in fine*). El Grupo de trabajo del artículo 29 no comprende la razón de tal exención y considera que la responsabilidad debería aplicarse también en este caso.

Falta de referencia al principio de limitación de la finalidad

El Grupo de trabajo del artículo 29 constata que el principio de responsabilidad de la transferencia ulterior (anexo II, Sec. II.3.) explica que los datos personales se pueden transferir a un tercero que actúe como agente exclusivamente para fines específicos y limitados, pero no indica explícitamente que esos fines concretos y limitados hayan de ser compatibles con los fines iniciales para los que fueron recogidos los datos, ni con las instrucciones del responsable del tratamiento. Se precisa una mayor transparencia a este respecto. Por consiguiente, el Grupo de trabajo del artículo 29 recomienda que se garantice que la Decisión de adecuación contiene información más detallada, por ejemplo, incluyendo una referencia clara al principio de limitación de la finalidad (anexo II, Sec. II.5.), según el cual los datos no se podrán tratar (ni divulgar) de manera incompatible con el principio de transferencia ulterior (además del principio de exclusión voluntaria).

Necesidad de obligaciones adicionales para las organizaciones del Escudo de la privacidad que actúen como encargados del tratamiento (agentes) en la transferencia ulterior de datos a otro encargado (agente)

La ausencia de normas claras para cuando la organización del Escudo actúe como agente (es decir, en nombre de un responsable del tratamiento de la UE) constituye un vacío y podría impedir que el responsable del tratamiento de la UE mantenga el control. Una organización del Escudo que reciba datos como agente de un responsable del tratamiento de la UE tiene que respetar las instrucciones del responsable del tratamiento de la UE. Ello se debería mencionar explícitamente en los principios, con el fin de garantizar que no respetar dichas instrucciones no solo dará lugar a un incumplimiento del contrato (anexo II, Sec. III.10.a.ii), sino también a una infracción de los principios del Escudo de la privacidad.

La posibilidad de que una organización del Escudo que actúe como agente realice una transferencia ulterior de datos a un tercero que actúe como agente debe ser transparente para el responsable del tratamiento y estará sujeta a su aprobación previa. Por tanto, debe establecerse claramente que es el contrato firmado por el agente con el responsable de la UE

(al que se hace referencia en la pregunta frecuente 10 como el «contrato del artículo 17») el que determina si se permite una transferencia ulterior[22].

Las condiciones actuales aplicables a la transferencia ulterior a un agente se basan en el supuesto de que la organización del Escudo actúa como responsable del tratamiento y, por tanto, puede decidir por sí misma sobre la posible intervención de un tercer agente. No obstante, esto no ha de ser posible cuando la organización del Escudo actúe como agente. De otro modo, el responsable del tratamiento de la UE se vería privado de sus capacidades de control.

Las disposiciones de privacidad correspondientes del contrato celebrado con un tercer agente deberán estar a disposición del responsable del tratamiento y ofrecerán al menos el mismo nivel de protección que el previsto en el contrato suscrito con el responsable del tratamiento.

2.2.4 Integridad de los datos y limitación de la finalidad

a) Proporcionalidad

En relación con una cuestión menor, el Grupo de trabajo del artículo 29 hace referencia a su carta dirigida a la Vicepresidenta Reding, en la que afirmó que «un tratamiento de datos personales podría, incluso en el marco de un respeto estricto de los principios de notificación y opción, ser desproporcionado respecto de los derechos y libertades del interesado o de la sociedad. El principio de proporcionalidad o de razonabilidad debe respetarse en todas las fases del tratamiento y debe aplicarse además a los principios de notificación y opción»[23].

El Escudo de la privacidad (anexo II, Sec. II.5.a.) establece que la información debe limitarse a lo pertinente para el tratamiento. El Grupo de trabajo del artículo 29 preferiría que esta frase se modificara en la Decisión de adecuación final, pues el mero hecho de que los datos sean pertinentes para el tratamiento no es suficiente para que el tratamiento sea proporcionado. Con el fin de cumplir el principio de proporcionalidad, el tratamiento debe limitarse a los datos que sean necesarios para el tratamiento de datos de que se trate.

b) Precisión

El principio de integridad de los datos y de limitación de la finalidad (anexo II, Sec. II.5.) establece también que «en la medida necesaria para alcanzar dichos fines, las entidades adoptarán medidas razonables para que los datos personales tengan fiabilidad para el uso previsto y sean exactos, completos y actuales.» El Grupo de trabajo del artículo 29 señala observar que es exactamente la misma redacción que se utiliza en el Acuerdo de puerto seguro. El Grupo de trabajo del artículo 29 duda que la expresión «en la medida necesaria para alcanzar dichos fines» deba incluirse, ya que, en su opinión, la exactitud de los datos no debe depender de la finalidad del tratamiento. El Grupo de trabajo del artículo 29 preferiría que en la Decisión de adecuación final no se efectúe esta vinculación entre exactitud y fines.

[22] Véase la carta del Grupo de trabajo del artículo 29 a la Vicepresidenta Reding de 10 de abril de 2014, punto 4 del epígrafe «Transferencia ulterior».
[23] Véase la carta del Grupo de trabajo del artículo 29 a la Vicepresidenta Reding de 10 de abril de 2014, p. 8.

c) Limitación de los fines

Cuando un responsable del tratamiento de datos establecido en la UE transfiera datos personales a una entidad estadounidense, el exportador de los datos deberá informar explícitamente a la entidad de los EE. UU. de los fines para los que se hayan recogido inicialmente. Esto es esencial para determinar si se produce un cambio de finalidad después de la transferencia, lo que desencadenaría la aplicación de los principios de notificación y opción y contribuiría a la asignación de riesgos y responsabilidades.

El principio de integridad de los datos y de limitación de la finalidad (anexo II, Sec. II.5.) dispone que una entidad no podrá tratar los datos personales de una manera incompatible con los fines para los que se recogieron o con fines autorizados posteriormente por el interesado. Sin embargo, el principio de opción (anexo II, Sec. II.2.) prevé el consentimiento expreso para el «uso» de la información delicada (es decir, la información personal que especifica condiciones de salud o sanitarias, origen racial o étnico, opiniones políticas, convicciones religiosas o filosóficas o pertenencia a un sindicato, o los datos que especifican la orientación sexual de la persona, así como los relativos a antecedentes penales) con fines sustancialmente diferentes de aquellos para los que los datos hayan sido recogidos inicialmente o que el interesado haya autorizado posteriormente. Este consentimiento expreso no es necesario en las situaciones mencionadas en el principio complementario 1.a. (anexo II, Sec. III.1.a.). Por lo que se refiere a datos personales que no son delicados, está previsto un régimen de exclusión voluntaria.

El Grupo de trabajo del artículo 29 señala que el ámbito de aplicación del principio de limitación de la finalidad es diferente con arreglo a los principios de notificación, de opción y de integridad de los datos y de limitación de la finalidad. En efecto, las expresiones «fin incompatible» y «fin sustancialmente diferente» se utilizan en el mismo texto sin una definición clara de estos dos conceptos[24].

El Grupo de trabajo del artículo 29 está muy preocupado por la posibilidad de que tal incoherencia dé lugar a grandes dificultades a la hora de conciliar el principio de integridad de los datos y de limitación de la finalidad (anexo II, Sec. II.5.) con el principio de opción (anexo II, Sec. II.2.), pues uno indica que los datos no pueden tratarse de manera incompatible con los fines para los que fueron recogidos, mientras que el otro contempla un mecanismo de exclusión voluntaria en caso de que los datos sean tratados con fines sustancialmente diferentes de la finalidad original.

De ello se deduce la posibilidad de interpretar que el principio de opción autoriza un tratamiento incompatible[25]. Según el Grupo de trabajo del artículo 29, debe establecerse

[24] El Grupo de trabajo del artículo 29 señaló que se utilizan otras expresiones: «la utilización no es coherente con» (anexo II, Sec. III.14.b.ii.), «utilizarla con fines diferentes» (anexo II, Sec. III.9.b.i.), «información para un fin distinto de aquel con el que inicialmente la recogió» (anexo II, Sec. II.1.b.). Esta falta de claridad podría dar lugar a una falta de garantías suficientes en relación con el principio de limitación de la finalidad.

[25] Véanse asimismo las observaciones que figuran en el principio de opción. El Grupo de trabajo del artículo 29 considera que el hecho de que las normas sobre transferencias ulteriores (anexo II, Sec. II.3.) solo se refieran al principio de opción y no al principio de limitación de la finalidad aumenta el riesgo de que así se entienda.

explícitamente que una entidad no estará autorizada a tratar datos con un fin sustancialmente diferente cuando ese fin sea incompatible con arreglo al principio de limitación de la finalidad. En otras palabras, debe quedar claro que el principio de opción no constituye una exención del principio de limitación de la finalidad.

En cualquier caso, si el tratamiento ulterior puede considerarse compatible, los principios de notificación y opción también deben aplicarse.

2.2.5 Excepciones periodísticas

Las excepciones periodísticas al tratamiento de datos personales están cubiertas por el principio complementario 2 (anexo II, Sec. III.2.). Se entiende que estas disposiciones reflejan la protección constitucional de los EE. UU. de la libertad de expresión. Por consiguiente, los documentos del Escudo de la privacidad indican que la información personal «que se recabe de material de archivo publicado anteriormente no estará sujeta a los requisitos de los principios del Escudo de la privacidad» (anexo II, Sec. III.2.b.). Esta exención parece incluir cualquier tratamiento posterior por un responsable o encargado del tratamiento de datos, es decir, no parece limitarse a un tratamiento posterior con fines periodísticos. Como ya se indicaba en la carta dirigida a la Vicepresidenta Reding el 10 de abril de 2014, el Grupo de trabajo del artículo 29 habría preferido un enfoque más limitado de las excepciones periodísticos, más en consonancia con el principio aplicado en la UE, así como con el derecho a la supresión a raíz del asunto Google Spain[26].

2.2.5 Derecho de acceso, corrección y supresión de los interesados

De conformidad con el Escudo de la privacidad, las personas tienen derecho a obtener la *confirmación* de si la entidad trata sus datos y a que *se les comuniquen* esos datos (anexo II, iii.8.a.i.). Sin embargo, la obligación de las entidades de responder a las solicitudes de los particulares relacionadas con las finalidades del tratamiento, las categorías de los datos personales en cuestión y los destinatarios o categorías de destinatarios a quienes se revelan los datos personales es bastante débil. El Grupo de trabajo del artículo 29 considera que los datos que se deben proporcionar al interesado han de mencionarse en el cuerpo del texto, en lugar de aparecer únicamente en una nota a pie de página, y que se han presentar como una obligación clara (relacionada con el anexo II, iii.8.a.i.1.).

Según el principio complementario 8, «el acceso debe facilitarse únicamente en la medida en que la entidad conserve información personal» (anexo II, iii.8.d.ii.). Esta norma no debe interpretarse de manera restrictiva, en el sentido de que en principio se debe dar acceso a todos los datos tratados por la entidad, independientemente del modo en que los haya tratado, y no solamente a los que haya almacenado. Por consiguiente, a efectos de la efectividad del derecho de acceso, es importante dejar claro que «almacenar» significa «tratar» en el sentido de la definición prevista en el anexo II, Sec.I.8.b. La aplicación de esta norma se debería examinar cuidadosamente durante la revisión conjunta del Escudo de la privacidad.

[26] Asunto C-131/12, Google Spain/Agencia Española de Protección de Datos y Mario Costeja González, 13 de mayo de 2014.

Sigue preocupando la lista de excepciones que se facilita en el anexo II, Sec. III.8.e.i., similar a la que se proporciona en la pregunta frecuente 8 del puerto seguro, a inclinar la balanza en favor de los intereses de las entidades. En este sentido, no se concederá a los particulares el acceso a sus propios datos personales, por los motivos siguientes: «vulneración de un privilegio o una obligación jurídica o profesional» (anexo II, Sec. III.8.e.3.), «perjuicio para las investigaciones sobre la seguridad de los empleados o los procedimientos de resolución de reclamaciones, o para la planificación de las sustituciones de los empleados y las reestructuraciones de las empresas» (anexo II, Sec. III.8.e.4.), y «perjuicio para la confidencialidad necesaria para las funciones de control, inspección o regulación relacionadas con la buena gestión financiera o en negociaciones futuras o en curso en las que participe la organización» (anexo II, Sec. III.8.e.5.). Al interpretar estos motivos debe tenerse presente la exención general relativa a la información comercial confidencial contenida en el anexo II, Sec. III.8.c. Por tanto, un particular nunca tendrá acceso a sus datos en las situaciones enumeradas anteriormente, al no lograrse un equilibrio entre los derechos e intereses de los particulares y los de la entidad para llegar a una solución sobre la solicitud de acceso.

El Grupo de trabajo del artículo 29 recuerda que las personas tienen derecho a acceder a sus propios datos en virtud del artículo 8, apartado 2, de la Carta. Aunque no se trata de un derecho absoluto, es fundamental para el derecho a la protección de los datos personales, pues facilita el ejercicio de otros derechos de los interesados, tales como la rectificación y supresión.

Por lo que se refiere a los derechos de rectificación y supresión, el Grupo de trabajo del artículo 29 acoge con satisfacción una mejora significativa conseguida por los principios del Escudo de la privacidad con respecto a los principios de puerto seguro, por la que dichos derechos se conceden no solo en las situaciones en las que los datos son inexactos, sino también si los datos se han tratado infringiendo los principios (anexo II, Sec. II.6.).

2.2.6 Recurso, aplicación y responsabilidad (mecanismos de recurso)

a) Ejercicio efectivo de los derechos de recurso de los ciudadanos de la UE

El Grupo de trabajo del artículo 29 reconoce los compromisos de las autoridades de EE. UU. en lo que respecta a los diferentes niveles del mecanismo de recurso. Sin embargo, dadas la complejidad y la falta de claridad de la arquitectura general del mecanismo, el Grupo de trabajo del artículo 29 teme que, en la práctica, el ejercicio efectivo de los derechos del interesado se vea menoscabado. El Grupo de trabajo del artículo 29 destaca que la calidad del mecanismo de recurso debe prevalecer sobre la cantidad de los mecanismos a disposición de las personas de la UE. También suscita preocupación que la mayoría, si no todos, los mecanismos de recurso prevean un procedimiento en los EE. UU., lo que complica el seguimiento del procedimiento por parte de las APD de la Unión Europea.

En efecto, el mecanismo de recurso previsto en el Escudo de la privacidad se centra, en primer lugar, en la posibilidad de que el interesado «reivindique sus derechos y prosiga el asunto de incumplimiento de los principios de privacidad mediante contactos directos con la

empresa autocertificada de los EE. UU.[27]». Por otra parte, las entidades deben designar un órgano de resolución de litigios independiente para investigar y resolver las reclamaciones individuales. El Grupo de trabajo del artículo 29 acoge con satisfacción el hecho de que ello se organice sin coste alguno para el particular.

Asimismo, se pueden presentar reclamaciones directamente a la Comisión Federal de Comercio, aunque esta no tiene la obligación de atenderlas. Una APD también podría remitir una reclamación. El DoC se ha comprometido a revisar y a hacer todo lo posible por facilitar la resolución de las reclamaciones (anexo I), a las que la Comisión Federal de Comercio concederá una consideración prioritaria (anexo II, Sec. III.7.e.). No obstante, la priorización de las reclamaciones por parte de la Comisión Federal de Comercio no ofrece certeza alguna al interesado de que sus reclamaciones se vayan a tratar.

En última instancia, los particulares tienen la posibilidad de invocar el arbitraje vinculante. El panel de arbitraje estará radicado en los EE. UU. y sus resoluciones serán recurribles ante los tribunales de los EE. UU.

El Escudo de la privacidad también ofrece la posibilidad de que la entidad opte por la cooperación con las APD de la Unión Europea (anexo II, Sec. III.5.a.). Esto es incluso obligatorio en el caso de los datos sobre recursos humanos recopilados en el marco de una relación laboral (anexo II, Sec. III.9.d.ii.). En tal situación, la resolución alternativa de litigios (RAL) no será aplicable (anexo II, Sec. III.5.a.). El Escudo de la privacidad no establece claramente cómo se organizará en la práctica la cooperación con las APD de la Unión Europea. En particular, no está claro si el panel se ocupará de todos los asuntos o si cada asunto diferente será examinado por un panel distinto.

El Grupo de trabajo del artículo 29 considera que es preciso detallar más en la Decisión de adecuación cuándo tienen competencia las APD para conocer las reclamaciones. Aparentemente esto depende de la cualificación de la entidad, pero no queda claro de qué manera.

Cuando la entidad actúe como agente en nombre de un responsable del tratamiento de la UE, los particulares tendrán en cualquier caso la posibilidad de presentar reclamaciones a la APD de la Unión Europea. La situación será similar para el tratamiento de los datos sobre recursos humanos y otros datos comerciales.

En caso de que la organización del Escudo de la privacidad actúe como responsable del tratamiento de datos, la competencia de una APD para tramitar la reclamación se limitará al tratamiento sujeto a la legislación de la UE (tratamiento bajo la responsabilidad del responsable de tratamiento de datos de la UE, incluida la responsabilidad conjunta con la entidad de los EE. UU., o cuando la organización del Escudo de la privacidad esté directamente sujeta a la legislación de la UE, por ejemplo mediante la utilización de equipos en la UE). No obstante, si el tratamiento de datos se efectúa en virtud únicamente de la legislación de los EE. UU., se aplicarán exclusivamente los mecanismos del Escudo de la

[27] Comisión Europea, proyecto de Decisión de adecuación, apartado 30.

privacidad. Con el fin de superar las barreras lingüísticas y la falta de conocimientos del ordenamiento jurídico de los EE. UU., podría ser útil que las APD de la Unión Europea tengan derecho a actuar como intermediarios en la reclamación presentada por un individuo, o a prestarle asistencia en los procedimientos RAL con entidades de los EE. UU. o durante sus contactos con las autoridades estadounidenses, si la APD lo considera apropiado.

El Grupo de trabajo del artículo 29 destaca que el mecanismo explicado en el Escudo de la privacidad no sigue la recomendación anterior, según la cual los ciudadanos de la UE han de poder presentar una demanda de indemnización por daños y perjuicios en la Unión Europea y han de tener derecho a presentar una demanda ante un órgano jurisdiccional nacional competente de la UE[28]. Convendría que las organizaciones del Escudo de la privacidad incluyesen tal posibilidad en sus políticas de privacidad.

A fin de garantizar la eficacia, el Grupo de trabajo del artículo 29 recomienda que el sistema permita a las APD de la Unión Europea representar al interesado y actuar en su nombre o como intermediario. En caso contrario, deberá contener una cláusula atributiva de competencia específica que permita a los interesados ejercer sus derechos en Europa.

b) Arbitraje

Los procedimientos de arbitraje final todavía no se han ultimado, lo que complica la evaluación al Grupo de trabajo del artículo 29. Dado que, al parecer, el sistema de arbitraje tendrá lugar en el marco de la legislación estadounidense y que la única lengua de procedimiento será el inglés, es posible que las APD de la Unión Europea deseen tener derecho a prestar asistencia a los particulares en el proceso.

Además, el procedimiento de arbitraje se ha establecido debido a la inseguridad de que la reclamación se llegue a tratar, pues la Comisión Federal de Comercio no tiene la obligación de tramitar todas las reclamaciones. El Grupo de trabajo del artículo 29 considera que, en caso de que un particular juzgue necesaria la asistencia de un abogado, tendrá que pagarle a este los honorarios correspondientes, lo cual puede impedir a los particulares someter sus reclamaciones al procedimiento de arbitraje.

c) Supervisión, aplicación y eficacia de los mecanismos de recurso

<u>Condiciones para participar en el Escudo</u>

Según el TJUE, la fiabilidad de un sistema de autocertificación «descansa, en esencia, en el establecimiento de mecanismos eficaces de detección y de control que permitan identificar y sancionar en la práctica las posibles infracciones de las reglas que garantizan la protección de los derechos fundamentales [...]»[29].

El Grupo de trabajo del artículo 29 señala que, en el marco del Escudo de la privacidad, el papel del DoC en el proceso de certificación parece reducirse a una mera verificación de la

[28] Véase la carta dirigida por el Grupo de trabajo del artículo 29 a la Vicepresidenta Reding, 10 de abril de 2014.
[29] TJUE, Schrems, apartado 81.

exhaustividad de los documentos. Aunque el Grupo de trabajo del artículo 29 constata que la autocertificación no implica un control sistemático *a priori* de la aplicación de las políticas de privacidad, el DoC debe, cuando menos, comprometerse a comprobar sistemáticamente que las políticas de privacidad incluyen todos los principios del Escudo de la privacidad. Este compromiso se menciona en el proyecto de Decisión de adecuación, pero no puede identificarse claramente en la carta de manifestaciones del DoC[30].

El incumplimiento de los principios del Escudo de la privacidad podría pasar inadvertido durante un largo período y no detectarse hasta que se haya producido un daño grave y posiblemente irreparable a los derechos fundamentales del interesado. Por tanto, este planteamiento podría vulnerar el principio de cautela europeo.

Transparencia por medio del Escudo de la privacidad y registro de entidades retiradas de la lista

Se han conseguido importantes mejoras en materia de transparencia con respecto al interesado. Además de todas las organizaciones estadounidenses autocertificadas ante el DoC, la nueva lista del Escudo de la privacidad contendrá un registro de todas las entidades retiradas de la lista del Escudo de la privacidad en la que se hará constar la razón por la que la entidad haya sido retirada[31]. El sitio web del Escudo de la privacidad del DoC se centrará más en el público destinatario de un modo que facilitará la verificación del tipo de información amparada por la autocertificación de una organización, así como la política de privacidad que se aplica a la información cubierta y el método que utiliza la organización para verificar su adhesión a los principios[32]. El Grupo de trabajo del artículo 29 acoge con satisfacción el hecho de que se haya expresado de manera explícita que el DoC comprobará si las empresas que disponen de sitios web públicos publican su política de privacidad en esos sitios web o, si no tienen sitios web públicos, dónde se pone la política de privacidad a disposición del público[33]. Además, los documentos ofrecen un mayor grado de información sobre el contenido de la política de privacidad[34].

El Grupo de trabajo del artículo 29 considera que se podría plantear un problema si una entidad ya incluida en la lista del Escudo de la privacidad amplía posteriormente su certificación a otras categorías de datos. En tales casos, la lista no reflejará los diferentes períodos de aplicabilidad de los principios a las diferentes categorías de datos. Ello entraña el riesgo de que los particulares y las empresas de la UE no puedan evaluar plenamente si un conjunto de datos específico está efectivamente sujeto a los principios del Escudo de la privacidad y, en caso afirmativo, desde cuándo. Con el fin de paliar esta deficiencia, el Grupo

[30] Comisión Europea, proyecto de Decisión de adecuación, apartado 34.
[31] Anexo I, p. 5 y anexo II, Sec. II.1.; el Grupo de trabajo del artículo 29 se remite asimismo a la cuarta recomendación de la Comisión en su Comunicación COM(2103)847, así como a la carta de 10 de abril de 2014 dirigida por el Grupo de trabajo del artículo 29 a la Vicepresidenta Reding, y en particular a su punto 5 del epígrafe «Transparencia».
[32] Anexo I, p. 8; el Grupo de trabajo del artículo 29 también hace referencia a su carta de 10 de abril de 2014 a la Vicepresidenta Reding, y en particular a su punto 2 del epígrafe «Transparencia».
[33] Anexo I, p. 3 y 4; el Grupo de trabajo del artículo 29 también hace referencia a la primera recomendación de la Comisión en su Comunicación COM(2103)847, así como a la carta de 10 de abril de 2014 dirigida por el Grupo de trabajo del artículo 29 de la Vicepresidenta Reding, y en particular a su punto 3 del epígrafe «Transparencia».
[34] Anexo I, p. 5 y 6 y anexo II, Sec. III.6.

de Trabajo recomienda que, para cada categoría de datos personales, se especifiquen separadamente en un registro de entidades de la lista del Escudo de la privacidad los datos relativos al comienzo de la aplicación de la autocertificación.

El Grupo de trabajo del artículo 29 acoge con satisfacción que el DoC vaya a llevar un registro de las entidades que se hayan retirado de la lista del Escudo de la privacidad y que ese registro vaya a contener una explicación que aclare que dichas entidades han dejado de gozar de los beneficios del Escudo de la privacidad, pero deben seguir aplicando los principios a los datos personales recibidos cuando eran entidades certificadas del Escudo de la privacidad mientras conserven esos datos (anexo I, p. 3). No obstante, dado que algunas de las entidades retiradas de la lista del Escudo de la privacidad podrían optar por devolver o suprimir los datos que hayan recibido en virtud del Escudo de la privacidad, mientras que otras los conservarán, es importante ofrecer a los particulares más transparencia en esta cuestión. Por consiguiente, el registro de empresas del DoC debe indicar si la entidad sigue en posesión de los datos personales recibidos en el marco del Escudo de la privacidad o si los ha devuelto o suprimido. En caso de que la entidad siga en posesión de dichos datos, el registro deberá declarar explícitamente que la entidad ha de seguir aplicando los principios a tales datos.

Por otra parte, el registro mantenido por el DoC deberá mencionar que estas entidades ya no gozan de los beneficios del Escudo de la privacidad en las nuevas transferencias, lo que significa que ya no están autorizadas a recibir datos personales procedentes de la UE en virtud de los principios.

Procedimientos de verificación

Para verificar que la autocertificación es eficaz en la práctica, las entidades pueden llevar a cabo una autoevaluación o revisiones externas del cumplimiento. El Grupo de trabajo del artículo 29 lamenta que solo se exija la formación de los trabajadores cuando la entidad opte por la verificación mediante autoevaluaciones (anexo II, Sec. III.7.c.). También parece que la necesidad de verificar que las políticas son precisas, completas, se exponen de manera destacada, se aplican y son accesibles solo es necesaria si la entidad opta por la revisión interna (autoevaluaciones) y que la revisión por un mecanismo externo se limita únicamente al cumplimiento de la política de privacidad de la entidad.

A posteriori

El Grupo de trabajo del artículo 29 acoge con satisfacción que la Comisión Federal de Comercio y el DoC estén investidos de poderes de investigación en los casos de reclamación. Además, el Grupo de trabajo del artículo 29 toma nota de que el DoC tendrá la posibilidad de efectuar verificaciones *ex officio*, en particular mediante el envío de cuestionarios. Sin embargo, el Grupo de trabajo del artículo 29 desea asegurarse de que un enfoque de estas características es suficiente para cumplir el requisito del TJUE de los mecanismos efectivos de detección y supervisión de las infracciones. De hecho, el Grupo de trabajo del artículo 29 sigue teniendo preguntas sobre las facultades exactas de las autoridades de ejecución de los EE. UU. en la realización de inspecciones *in situ* en los locales de las entidades

autocertificadas para investigar las infracciones del Escudo de la privacidad, sobre cómo se puede obtener el *exequatur* de la decisión de una autoridad de la UE en territorio de los EE. UU., y sobre si las sanciones impuestas en virtud del Escudo de la privacidad son disuasorias en la práctica.

2.2.7 Tratamiento de datos sobre recursos humanos

Ámbito de aplicación

El principio complementario 9 (anexo II, Sec. III.9.) se aplica a la información personal de un trabajador (pasada o presente) obtenida en el contexto de la relación laboral. A tenor del principio complementario 9.a.ii., los principios del Escudo de la privacidad solo se aplican cuando se transfieren registros identificados o se accede a ellos. La expresión «registros identificados» no está en consonancia con la definición de la expresión «datos personales» recogida en el anexo II, Sec.I.8.a., que comprende los «datos referidos a una persona identificada o identificable» y, por lo tanto, no es acorde con la definición utilizada en la Directiva[35].

El principio complementario 9.a.ii. establece que «los informes estadísticos basados en datos agregados sobre empleo que no contengan datos personales o el uso de datos anónimos no plantean problemas en cuanto al derecho a la vida privada». Esta afirmación contradice una serie de dictámenes emitidos por el Grupo de trabajo del artículo 29. El Grupo de trabajo del artículo 29 desea destacar que los datos agregados se pueden volver a identificar y, por consiguiente, deben considerarse datos personales[36].

Notificación, opción y limitación de la finalidad

El principio complementario 9.b.i. constituye un ejemplo de aplicación de los principios de notificación y opción en el que los datos sobre recursos humanos se usan con fines diferentes. El ejemplo se refiere a una entidad estadounidense que desee «utilizar la información personal obtenida a través de la relación laboral para fines no relacionados con los laborales, como comunicaciones de márketing». En este escenario, el cambio de finalidad está autorizado siempre que respete el principio de notificación y opción. Según el Grupo de trabajo del artículo 29, el tratamiento ulterior de datos sobre recursos humanos para fines de mercadotecnia directa se deberá considerar, en la mayoría de los casos, un fin incompatible y, por lo tanto, contrario al principio de limitación de la finalidad (anexo II, Sec. II.5.a.). Además, el Grupo de trabajo del artículo 29 considera que la opción no puede ser una base apropiada para que el trabajador dé su consentimiento («exclusión voluntaria») a un cambio de finalidad, en el contexto del empleo, cuando dicho consentimiento pueda no ser enteramente libre.

[35] Como ya se ha subrayado, la limitación a los registros que se transfieren o a los que se accede tampoco se ajusta al término «tratamiento» (anexo II, Sec. I.8 b.).
[36] Véase el Dictamen 4/2007 sobre el concepto de datos personales, así como el Dictamen 05/2014 sobre técnicas de anonimización.

El Grupo de trabajo del artículo 29 tiene serias dudas de que el enfoque principal del Escudo de la privacidad hacia el principio de opción como condición para el uso ulterior de los datos con fines distintos cumpla las Directrices sobre intimidad de la OCDE, pues no hay garantías suficientes para evitar que este mecanismo de exclusión voluntaria también pueda utilizarse para un tratamiento ulterior incompatible. El principio complementario 9.b.iv. prevé una exención explícita y amplia de los principios de notificación y opción en la medida y tiempo necesarios para que no haya perjuicio de los intereses legítimos de la entidad «cuando tome decisiones sobre ascensos, nombramientos y otras decisiones laborales similares». En primer lugar, el uso de datos sobre recursos humanos ya se debe mencionar explícitamente en el momento de la recogida de los datos. Por otra parte, el concepto de «otras decisiones laborales similares» es demasiado vago y general. Como consecuencia, cuando los datos sobre recursos humanos se traten en el marco de la relación laboral quedarán totalmente exentos del principio de notificación y opción. La expresión es tan amplia que no permite apreciar si el uso ulterior es compatible con la finalidad original. El Grupo de trabajo del artículo 29 recomienda la supresión de esta excepción.

Derecho de acceso

El principio complementario 9.e.i. también prevé una exención de la aplicación del principio de acceso o de la celebración de un contrato con un tercero responsable de datos sobre recursos humanos cuando se trate de necesidades operativas ocasionales relacionadas con el empleo, como la reserva de un vuelo, de una habitación de hotel o la cobertura de un seguro, que permite efectuar transferencias de datos personales de un pequeño número de empleados, siempre que se observen los principios de notificación y opción. El Grupo de trabajo del artículo 29 no ve ninguna justificación razonable para dicha exención y recomienda que se suprima ese apartado.

2.2.8 Productos médicos y farmacéuticos

Ámbito de aplicación

El Escudo de la privacidad considera que las transferencias de datos codificados desde la Unión Europea a los EE. UU. en el contexto de los productos médicos y farmacéuticos no constituye una transferencia sujeta al Escudo de la privacidad (anexo II, Sec. III.14.g.i.). Sin embargo, la transferencia de datos codificados goza de protección en virtud de la normativa europea de protección de datos. Esto significa que, en la práctica, el Escudo de la privacidad no puede cubrir dichas transferencias. El Grupo de trabajo del artículo 29 insta a la Comisión de la UE a proponer explícitamente que el proyecto de Decisión de adecuación no cubra la transferencia de datos codificados por motivos médicos o farmacéuticos y que estas transferencias queden cubiertas por otras salvaguardias, como cláusulas contractuales tipo o normas vinculantes para las empresas. El Grupo de trabajo del artículo 29 propone que este punto se precise en la Decisión de adecuación final.

Transferencias con fines de regulación y control (anexo II, Sec. III.14.d.)

El Grupo de trabajo del artículo 29 está preocupado porque, en virtud de estas disposiciones, datos personales recogidos por razones médicas y en su mayoría de carácter delicado puedan transferirse a las autoridades de regulación de los EE. UU. Dado que el Escudo de la privacidad está diseñado para las transferencias de datos entre entidades privadas, un organismo público como una autoridad de regulación de los EE. UU. no puede autocertificarse en virtud del Escudo de la privacidad, lo que suscita la cuestión de la protección de datos adecuada para dichas transferencias. En caso de que tales transferencias deban administrarse con fines reguladores, se deberán adoptar medidas adecuadas para asegurar la continuidad de la protección de los derechos fundamentales del interesado. El Grupo de trabajo del artículo 29 hace hincapié en que el proyecto de Decisión de adecuación no contempla ninguna apreciación sobre este punto. Por consiguiente, el Grupo de trabajo del artículo 29 no tiene ninguna garantía de que los datos delicados de interesados de la UE gocen de una protección adecuada en este contexto.

Además, el Grupo de trabajo del artículo 29 señala que no comprende por qué el objetivo del *marketing* figura como ejemplo de tratamiento para futuras investigaciones científicas. Por otra parte, la razón de que se autoricen transferencias ulteriores a filiales de empresas y otros investigadores (anexo II, Sec. III.14.d.) de la rúbrica «Transferencias con fines de regulación y control» no está clara. Estas cuestiones requieren una aclaración en la Decisión de adecuación final.

Control de la eficacia y la seguridad de los productos (incluida la información a organismos públicos) y seguimiento de los pacientes que utilicen determinadas medicinas o dispositivos médicos

El Escudo de la privacidad prevé una exención a los principios de notificación, opción, transferencia ulterior y acceso en la medida en que la adhesión al principio interfiera en el cumplimiento de los requisitos normativos. El proyecto de Decisión de adecuación no contempla ninguna conclusión por lo que se refiere a la situación en que los principios de la privacidad interfieran en el cumplimiento de los requisitos reglamentarios. Aunque el Grupo de trabajo del artículo 29 podría entender que las investigaciones de los gobiernos puedan justificar límites a la notificación y al derecho de acceso para la protección de las investigaciones, el Grupo no ve razones que puedan justificar estas amplias exenciones cuando están llevando a cabo el tratamiento una entidad o un tercero del sector privado. Por ejemplo, dado que el tratamiento de los pacientes es cada vez más individualizado, dicha amplia exención de los principios de privacidad en caso de seguimiento de los pacientes que utilizan determinadas medicinas o dispositivos médicos es inaceptable, pues este tipo de asistencia se convertirá en una práctica común. Esto también es pertinente cuando las empresas farmacéuticas utilizan los datos para el control de la eficacia y la seguridad de los productos (ensayo o venta de nuevos medicamentos).

2.2.9 Información accesible al público

La excepción al derecho de acceso en caso de información accesible al público e información de registros públicos (anexo II, Sec. III.15.d. y e.) suscita dudas en los casos en que a un

particular, al ejercer su derecho de acceso, le interesa saber si un responsable del tratamiento determinado trata sus datos y qué datos se están tratando, con el fin de poder controlar el tratamiento de sus datos. El Grupo de trabajo del artículo 29 ha declarado en repetidas ocasiones que, con arreglo a la legislación de la UE, los interesados gozan siempre del derecho a acceder a sus datos y, en su caso, a exigir la rectificación o supresión de los datos cuando estos no se hayan tratado de manera lícita o si son incompletos o inexactos, independientemente de que los datos personales hayan sido publicados o no[37]. Si la solicitud de acceso del particular se rechaza porque los datos se han obtenido de fuentes de acceso público o registros públicos, el interesado perderá la capacidad de controlar la exactitud de los datos y de averiguar si, en un primer momento, los datos se hicieron públicos lícitamente.

No obstante, el Escudo de la privacidad exime la información de registros públicos y la información accesible al público de los principios de notificación, opción, acceso y responsabilidad por una transferencia ulterior (anexo II, Sec. II.15.b.). Estas exenciones parecen demasiado amplias en comparación con las de la Directiva y suscitan preocupación, ya que menoscaban, entre otras cosas, las posibilidades de los particulares de controlar la exactitud de sus datos y restringir la difusión de los mismos.

2.3 Conclusiones

El Grupo de trabajo del artículo 29 reconoce que las autoridades estadounidenses y la Comisión Europea han aportado importantes mejoras en los aspectos comerciales de la transferencia de datos entre los dos continentes. Sin embargo, teniendo en cuenta el análisis anterior, el Grupo de trabajo del artículo 29 considera que la parte comercial del Escudo de la privacidad requiere una mayor clarificación en numerosos puntos. Por ejemplo, la falta de un principio explícito de conservación de datos es motivo de preocupación. Por consiguiente, el Grupo de trabajo del artículo 29 tiene serias dudas de que el Escudo de la privacidad pueda garantizar un nivel de protección sustancialmente equivalente al de la UE.

La Decisión de adecuación ha de aclarar en mayor medida los principios de limitación de la finalidad y de opción. Existe riesgo de lagunas en relación con varios principios, en particular en lo referente a las transferencias ulteriores, el mecanismo de tramitación de reclamaciones y el tratamiento de los datos sobre recursos humanos o los datos farmacéuticos. Además, la manera en la que se van a aplicar los principios del Escudo de la privacidad a los encargados del tratamiento (agentes) requiere una mayor elaboración y se ha de prestar una atención especial para garantizar una aplicación clara e inequívoca de la terminología.

[37] Véase WP20, p. 4.

3. EVALUACIÓN DE LAS GARANTÍAS DE SEGURIDAD NACIONAL DEL PROYECTO DE DECISIÓN DE ADECUACIÓN

3.1 Garantías y limitaciones aplicables a las autoridades de seguridad nacional de los EE. UU.

Las injerencias en los derechos fundamentales a la vida privada y la protección de datos pueden ser admisibles, siempre que estén justificadas en una sociedad democrática. Esto significa que los principios de la privacidad no son absolutos y que las excepciones son posibles, pero solo si se satisfacen las garantías (esenciales) aplicables. A fin de ser coherentes con el objetivo de mejorar la protección de la vida privada, las entidades deberán además esforzarse en aplicar los principios de manera completa y transparente, lo que implica indicar en sus políticas de protección de la vida privada cuándo se aplicarán de manera regular las limitaciones a los principios permitidas por el ordenamiento jurídico de los EE. UU. Por esta misma razón, cuando se permita la opción a tenor de los principios y/o de la legislación de los EE. UU., se espera que las entidades opten por el mayor nivel de protección posible.

En el anexo II, Sec. I.5. se establece que «la observancia de los principios de privacidad «puede verse limitada por: a) exigencias de seguridad nacional, interés público y cumplimiento de la ley; b) por disposición legal o reglamentaria, o por jurisprudencia que origine conflictos de obligaciones o prevea autorizaciones explícitas, siempre que las entidades que recurran a tales autorizaciones puedan demostrar que el incumplimiento de los principios está limitado a la medida necesaria para garantizar los intereses legítimos esenciales contemplados por las mencionadas autorizaciones; o c) por excepción o dispensa prevista en la Directiva o las normas de Derecho interno de los Estados miembros siempre que tal excepción o dispensa se aplique en contextos comparables.

La cuestión que se plantea es si las excepciones mencionadas en el anexo II están justificadas en una sociedad democrática. Según el proyecto de Decisión de adecuación del Escudo de la privacidad, la Comisión concluyó que «en los EE. UU. existen normas destinadas a garantizar que las posibles injerencias cometidas a efectos de seguridad nacional en los derechos fundamentales de las personas cuyos datos personales se transfieran desde la Unión a los EE. UU. en el marco del Escudo de la privacidad UE-EE. UU. se limiten a lo estrictamente necesario para alcanzar el objetivo legítimo perseguido»[38].

Aplicando el marco como se establece en la sección 1.2 del presente dictamen y teniendo en cuenta las observaciones de las autoridades estadounidenses y las conclusiones de la Comisión, el Grupo de trabajo del artículo 29 ha evaluado el actual marco jurídico y las prácticas de las agencias de inteligencia de los EE. UU., así como las condiciones en las que permiten la existencia de injerencias en los derechos fundamentales al respeto de la vida privada y a la protección de datos tal y como quedan protegidos por el marco jurídico

[38] Proyecto de Decisión de la Comisión con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU., apartado 75.

europeo. Esta valoración se basa en el análisis de la Directiva de Política Presidencial 28 (PPD-28), el Decreto n.º 12333 (EO12333) y las distintas bases jurídicas establecidas por la Ley de inteligencia exterior (FISA, artículos 104, 402, 215, 501 y 702). El Grupo de trabajo del artículo 29 se ha basado en el anexo VI del Escudo de la privacidad, que consiste en un escrito preparado por la Oficina del Director de la Inteligencia Nacional (ODNI) en relación con las salvaguardias y limitaciones aplicables a las autoridades de seguridad nacional de los EE. UU. que resume la información proporcionada a la Comisión Europea en relación con las actividades de recopilación de inteligencia de señales de los EE. UU.

3.2 Garantía A: Necesidad de que el tratamiento esté previsto por la ley y se base en normas claras, precisas y accesibles

Según la legislación europea, las injerencias deben ser conformes a las leyes y a las políticas y los procedimientos establecidos y suficientemente claras y accesibles (dentro del margen de apreciación concedido a cada país) para dar a los ciudadanos una indicación adecuada de las circunstancias y las condiciones en las que las autoridades públicas están facultadas para recurrir a las medidas de vigilancia[39].

El Grupo de trabajo del artículo 29 constata que las actividades de inteligencia de señales se realizan sobre la base de un marco legal accesible. Todas las leyes mencionadas en el anexo VI (PPD-28, FISA, Ley de libertades de los EE. UU., FOIA) están disponibles en línea para el público en general (dentro y fuera de los EE. UU.). El anexo VI presenta un resumen del marco jurídico establecido, las limitaciones de la recogida, las limitaciones de la conservación y la difusión, el cumplimiento y la supervisión, la transparencia y las vías de recurso. El régimen jurídico de las actividades de inteligencia de los EE. UU. consiste en una serie de documentos que incluyen informes de las agencias individuales, políticas y procedimientos que deben analizarse para comprender mejor cómo se llevan a cabo las actividades, tanto en la teoría como en la práctica. A este respecto, el Grupo de trabajo del artículo 29 se ha concentrado en un número limitado de aspectos que considera esenciales.

3.2.1 Decreto n.º 12333 y Directiva de Política Presidencial 28

El ámbito de aplicación del EO12333 es amplio; en principio, se permite toda recogida de datos de inteligencia extranjera a discreción del Presidente de los EE. UU. sobre la base del Decreto. Sin embargo, se ha afirmado que, desde la introducción de la FISA, el EO12333 solo puede utilizarse para la recogida de datos fuera del territorio de los EE. UU. El Grupo de

[39] TEDH, Zakharov, apartado 247: «El Tribunal ya ha declarado que el requisito de "previsibilidad" de la Ley no es tan estricto como para obligar a los Estados a adoptar disposiciones legales en las que se enumeren con detalle todas las actuaciones que puedan dar lugar a la decisión de someter a un particular a vigilancia secreta por motivos de "seguridad nacional". Por la propia naturaleza de las cosas, el carácter de las amenazas a la seguridad nacional puede variar y dichas amenazas pueden ser imprevistas o difíciles de definir por adelantado (véase Kennedy, antes citado, apartado 159). Al mismo tiempo, el Tribunal ha subrayado también que en las cuestiones relacionadas con los derechos fundamentales, sería contrario a los principios del Estado de Derecho, que es uno de los principios básicos de una sociedad democrática consagrados en la Convención, que una facultad de apreciación concedida al poder ejecutivo en el ámbito de la seguridad nacional se expresase en términos de un poder sin restricciones. En consecuencia, la ley debe señalar, con suficiente claridad, el ámbito de dicho poder discrecional conferido a las autoridades competentes y las modalidades de su ejercicio, teniendo en cuenta el objetivo legítimo de la medida en cuestión, a fin de proporcionar a las personas una protección adecuada frente a una injerencia arbitraria».

trabajo del artículo 29 señala que el EO12333 no da muchos detalles en cuanto a su ámbito geográfico, la medida en la que los datos pueden recopilarse, conservarse y difundirse posteriormente, ni sobre la naturaleza de los delitos que pueden dar lugar a la vigilancia o el tipo de información que se puede recopilar o utilizar.

Según entiende el Grupo de trabajo del artículo 29, la finalidad principal de la Directiva de Política Presidencial 28 (Presidential Policy Directive, PPD-28) es establecer los límites de la recogida y el tratamiento de los datos personales, sean cuales sean el programa de vigilancia utilizado y el lugar donde se han obtenido los datos.

La PPD-28 es una Directiva del Presidente de los EE. UU. por la que se establecen los principios de coherencia con la recogida de inteligencia de señales que se deberá autorizar y efectuar, pero la PPD-28 no constituye una base jurídica para la recogida. La PPD-28 surte sus efectos mediante la imposición de dichos principios a los organismos de los servicios de inteligencia para incorporarlos a sus políticas y procedimientos. La Directiva se aplica a actividades de inteligencia de señales, con independencia de la ubicación de los datos en el momento en que se recojan, dentro o fuera de los EE. UU. Por lo tanto, también es aplicable a los datos recogidos para fines de inteligencia de señales cuando se transfieren desde la UE a los EE. UU.

En particular, la PPD-28 afirma que las actividades de inteligencia de señales deberán ser lo más adaptadas posible[40]. En cuanto a la utilización de los datos, establece procedimientos de minimización (incluidas las condiciones para su conservación y difusión), seguridad y acceso por el personal pertinente (es decir, las normas que contienen salvaguardias para limitar el riesgo de abuso y uso indebido), calidad y supervisión. Estas garantías se aplican con independencia de la nacionalidad de los interesados, es decir, a personas estadounidenses y no estadounidenses indistintamente.

Durante la transmisión de los datos a los EE. UU., las salvaguardias establecidas por la PPD-28 también son de aplicación. El anexo VI contiene el compromiso de la ODNI de que si los servicios de inteligencia de los EE. UU. han de recoger datos de los cables transatlánticos mientras se transmiten a los EE. UU., lo harán «con sujeción a las limitaciones y salvaguardias establecidas en el presente compromiso, incluidos los requisitos de la PPD-28»[41]. El Grupo de trabajo del artículo 29 constata que sigue sin haber jurisprudencia reiterada que determine la legalidad de la interceptación de cables en caso de que algún país la fuese a llevar a cabo. De todos modos, los EE. UU. ni confirman ni niegan que interceptan cables como medio para la recogida de datos de inteligencia.

El concepto de «inteligencia de señales» no se define en la PPD-28 ni en ningún otro texto aplicable.

[40] «Las actividades de inteligencia de señales deberán ser lo más adaptadas posible. Para determinar si se han de recoger datos de inteligencia de señales, los Estados Unidos tendrán en cuenta la disponibilidad de otras informaciones, incluso procedentes de fuentes diplomáticas y públicas. Se deberá dar prioridad a tales alternativas viables y adecuadas de inteligencia de señales» [artículo1, letra d)].

[41] Escudo de la privacidad, Anexo VI, carta de la Oficina del Director de Inteligencia Nacional (ODNI) relativa a las salvaguardias y limitaciones aplicables a las autoridades de seguridad nacional de los EE. UU., p. 2.

3.2.2 Ley de vigilancia de la inteligencia exterior

En general, el texto de la Ley de vigilancia de la inteligencia exterior (FISA) parece más claro y preciso. Sin embargo, la interpretación de varias disposiciones a la luz de la PPD-28 y, por ende, su aplicación práctica dependen en gran medida de la ejecución de las distintas agencias. Aunque aún no se dispone de un informe completo de la aplicación de las nuevas salvaguardias, los delegados de los EE. UU. han informado a los representantes del Grupo de trabajo del artículo 29 de que la aplicación de las salvaguardias de la PPD-28 se ha completado y se lleva a cabo de forma similar en todos los servicios de inteligencia de los EE. UU.

Más concretamente, el artículo 501 establece de manera relativamente clara el tipo de operaciones de inteligencia que se pueden ordenar: «la presentación de objetos tangibles (incluidos libros, registros, papeles, documentos y otros elementos)». Con todo, cabe señalar que la inclusión de «otros elementos» en la definición de «objetos tangibles» confiere al alcance de dicha autoridad un carácter bastante amplio.

El artículo 702, que permite recopilar datos de personas no estadounidenses de las que se crea razonablemente que se encuentran fuera de los EE. UU. a fin de obtener información de inteligencia extranjera[42], no presenta el mismo nivel de detalle que el artículo 501. En cuanto a su alcance, el artículo 702 se orienta a los prestadores de servicios de comunicaciones electrónicas establecidos en los EE. UU. para la recopilación de información de inteligencia exterior de particulares que se encuentren fuera de los EE. UU. La definición de «información de inteligencia exterior» es amplia. El documento incluye, entre otras cosas, «información en relación con una potencia extranjera o territorio extranjero que guarde relación con la política en materia de asuntos exteriores de los EE. UU.»[43], lo cual suscita cierta incertidumbre en cuanto al tipo de información que puede recogerse en la práctica.

A pesar de la desclasificación de documentos, informes al Congreso e informes del Consejo de supervisión de las libertades civiles y de la privacidad (en lo sucesivo, el PCLOB, por sus siglas en inglés), la aplicación de la FISA, incluidos su alcance y la utilización de términos de selección especificados, sigue siendo equívoca y confusa. La utilización de términos de selección especificados («selectores asignados») se menciona en un informe del PCLOB[44], pero el Grupo de trabajo del artículo 29 entiende que ello no se corresponde con las normas de segmentación establecidas con arreglo al artículo 702[45]. No se hace referencia en las normas accesibles al público en general, en la medida en que el Grupo de trabajo del artículo 29 lo ha podido confirmar.

[42] Código de los EE. UU., título 50, apartado 1881a (D) (1).
[43] Código de los EE. UU., título 50, apartado 1801 (e) (2).
[44] Informe del PCLOB sobre el programa de vigilancia ejecutado en virtud del artículo 702 de la FISA, p. 32.
[45] Código de los EE. UU., título 50, apartado 1881a (D).

3.2.3 Conclusión

En conjunto, el Grupo de trabajo del artículo 29 señala que los textos aplicables relativos a actividades de inteligencia están disponibles en línea y que las autoridades estadounidenses han tomado una serie de medidas importantes en pos de la transparencia.

El Grupo de trabajo del artículo 29 reconoce que desde 2013 se ha publicado un gran número de documentos, como medidas, procedimientos, decisiones del FISC y otros documentos desclasificados. Por otra parte, el PCLOB ha publicado informes importantes sobre las actividades realizadas sobre la base del artículo 702 y la Ley de libertades de los EE. UU. (USA Freedom Act). Se espera un informe similar sobre las actividades realizadas en virtud del EO12333.

Se han clasificado varios anexos legislativos que podrían arrojar luz sobre las implicaciones del Decreto para los particulares de fuera de los EE. UU. y las salvaguardias aplicables, y por tanto no son accesibles al público ni los particulares que pueden verse afectados por su aplicación. Cuando se ha desclasificado algún texto, el valor y la información sobre las actividades de inteligencia que aportan son limitados.

A pesar del esfuerzo realizado para explicar el funcionamiento del EO12333 tras las revelaciones de Snowden, en particular mediante la adopción de la PPD-28, la aplicación práctica de EO12333 sigue estando poco clara. El Grupo de trabajo del artículo 29 constata que el anexo VI del Escudo de la privacidad no aporta información detallada sobre el funcionamiento del EO12333.

Aunque el Grupo de trabajo del artículo 29 acoge con satisfacción las limitaciones incluidas en la PPD-28, resulta difícil saber si el marco jurídico para la vigilancia de los EE. UU. es suficientemente previsible, es decir, contiene «indicaciones suficientes en cuanto a las circunstancias y las condiciones en las que las autoridades públicas están facultadas para recurrir a tales medidas» mientras sigue pendiente una explicación más clara, incluida la publicación del informe del PCLOB en el EO12333.

3.3 Garantía B: Obligación de demostrar la necesidad y la proporcionalidad en relación con los objetivos legítimos perseguidos

3.3.1 Directiva de Política Presidencial 28

La PPD-28 introdujo limitaciones en relación con los fines para los que pueden utilizarse los datos personales y las condiciones en las que pueden difundirse y repercute en la recopilación de inteligencia de señales, independientemente del fundamento jurídico aplicado.

En particular, el artículo 1 la PPD-28 dispone que las actividades de inteligencia de señales siempre deben ser «lo más adaptadas posible». Aun reconociendo esta limitación, es difícil determinar si «lo más adaptadas posible» significa que toda recopilación de datos es necesaria y proporcionada.

La PPD-28 reconoce que la recopilación en bloque sigue estando permitida «con el objeto de identificar las amenazas nuevas o emergentes y otra información vital de seguridad nacional que a menudo se esconde dentro del enorme y complejo sistema de las comunicaciones globales modernas»[46]. El Grupo de trabajo del artículo 29 señala que la PPD-28 afirma que «inteligencia de señales recopilada en bloque significa la recopilación autorizada de grandes cantidades de datos de inteligencia de señales que, debido a consideraciones técnicas u operativas, se adquieren sin utilizar discriminantes (como identificadores específicos, términos de selección, etc.)».

La PPD-28 impone límites a la utilización de inteligencia de señales recogida en bloque en lo que se refiere a la finalidad de la utilización. Hay seis fines para los que se admite la recopilación «en bloque», que incluyen la lucha contra el terrorismo y otras formas de delitos graves (transnacionales). Del análisis del Grupo de trabajo del artículo 29 se desprende que la limitación de la finalidad es más bien amplia (posiblemente, demasiado amplia) para que se pueda considerar selectiva.

La PPD-28 no ha eliminado la posibilidad de recogida indiscriminada de datos personales en bloque y la escala de dichas posibilidades de recogida sigue sin estar clara y siendo potencialmente amplia. A este respecto, el Grupo de trabajo del artículo 29 señala que, en el anexo VI, la ODNI afirma que «las actividades de recopilación en bloque relacionadas con las comunicaciones por Internet que realizan los servicios de inteligencia estadounidenses a través de la inteligencia de señales operan en una pequeña parte de Internet»[47], por lo que agradecería más pruebas a través de medidas de transparencia.

3.3.2 Ley de vigilancia de la inteligencia exterior

En los artículos 215 y 702 de la FISA se introdujeron procedimientos de minimización con el fin de proteger a las personas de EE. UU. de un acceso de gran alcance a sus datos por parte del Gobierno. Estas limitaciones no se aplican a los extranjeros oficialmente, a pesar de que funcionarios del Gobierno de los EE. UU. han manifestado en repetidas ocasiones en reuniones tanto públicas como privadas con representantes del Grupo de trabajo del artículo 29 que, en la práctica, el ámbito de aplicación de los procedimientos de minimización se ha hecho extensivo a todas las personas, independientemente de su nacionalidad y de su lugar de residencia habitual.

El artículo 702 especifica que una adquisición autorizada «deberá llevarse a cabo de manera coherente con la Cuarta Enmienda a la Constitución de los EE. UU., que limita la recogida de datos a lo que se considere conforme con el principio de búsqueda razonable. A este respecto, no se realiza ninguna distinción entre empresas estadounidenses y empresas no

[46] PPD-28, artículo 2, y Escudo de la privacidad, anexo VI, carta de la Oficina del Director de Inteligencia Nacional (ODNI) relativa a las salvaguardias y limitaciones aplicables a las autoridades de seguridad nacional estadounidenses, p. 3.
[47] Escudo de la privacidad, anexo VI, carta de la Oficina del Director de Inteligencia Nacional (ODNI) relativa a las protecciones y limitaciones aplicables a las autoridades de seguridad nacional estadounidenses, p. 4. El Grupo de trabajo del artículo 29 recuerda a este respecto el informe de las conclusiones de los Copresidentes de la UE del Grupo de trabajo *ad hoc* UE-EE. UU. sobre protección de datos, que afirma que «los datos de comunicaciones representan una parte muy pequeña del tráfico global de Internet», dado que «la mayor parte del tráfico global de Internet está formada por un elevado volumen de retransmisiones y descargas, como series de televisión, películas y deportes» (punto 3.1.2 del informe).

estadounidenses». En otras palabras, si la Cuarta Enmienda se aplicara a todos los datos recopilados en los EE. UU., la recogida «en bloque» en los EE. UU. sería «desproporcionada» y, por tanto, inconstitucional.

El Grupo de trabajo del artículo 29 acoge con satisfacción las conclusiones del informe del PCLOB, según las cuales «en la práctica, las "personas no estadounidenses" también se benefician de las restricciones al acceso y la retención exigidas por los procedimientos de minimización o segmentación de las diferentes agencias, pues el coste y la dificultad de identificar y suprimir la información de las personas de los EE. UU. en un amplio corpus de datos hacen que normalmente todo el conjunto de datos se maneje de acuerdo con los más altos estándares de datos estadounidenses».

El Grupo de trabajo del artículo 29 señala que, atendiendo a las conclusiones de PCLOB, «el programa no se ejecuta mediante la recopilación de comunicaciones en bloque». El Informe estadístico de transparencia de 2014 publicado por la ODNI confirma esta conclusión. Además, según el informe del PCLOB, se utilizan «selectores asignados», como direcciones de correo electrónico o números de teléfono, para orientar la vigilancia[48].

Sin embargo, las normas públicas disponibles relativas a la segmentación no prevén estas normas selectivas y solo tienen por objeto evitar la segmentación de las personas estadounidenses o que se encuentran en los EE. UU. Por otra parte, los beneficios que según el PCLOB se aplican en la práctica a las personas no estadounidenses no son jurídicamente vinculantes y no están legalmente establecidos, ya que la disposición normativa en materia de segmentación no prevé tales normas selectivas y solo tiene por objeto evitar la segmentación de los ciudadanos estadounidenses y las personas que se encuentran en los EE. UU.

El Grupo de trabajo del artículo 29 recuerda asimismo que, a efectos del artículo 702, las personas no son solo los particulares, sino también los grupos, entidades, asociaciones, sociedades y potencias extranjeras. Por otra parte, el hecho de que la recogida se justifique con que uno de los principales fines de la recopilación de datos sea obtener información de inteligencia exterior deja cierta incertidumbre acerca de sus fines y su necesidad. Sin embargo, el Grupo de trabajo del artículo 29 acoge con satisfacción la información facilitada en el anexo VI según la cual el número total de afectados por el artículo 702 en 2014 fue de aproximadamente 90 000 personas[49]. La primera revisión del Escudo de la privacidad brindará la oportunidad de que se presenten pruebas complementarias de las normas de segmentación.

Hasta la fecha, no existe una jurisprudencia concluyente sobre la legalidad de la recogida de datos masivos e indiscriminados y la posterior utilización de los datos personales con fines de lucha contra la delincuencia, incluida la cuestión de en qué circunstancias pueden tener lugar la recopilación y el uso de datos personales. Se espera que el TJUE aborde esta cuestión, al menos en cierta medida, en el transcurso de 2016, tanto en los asuntos acumulados Tele2 Sverige AB/Post- och telestyrelsen y Secretary of State for the Home Department/Davis y

[48] Informe del PCLOB sobre el programa de vigilancia ejecutado en virtud del artículo 702 de la FISA, p. 32.
[49] Anexo VI, p. 11.

otros[50], como en el asesoramiento sobre la validez del Acuerdo UE-Canadá sobre el PNR[51]. Entretanto, el Grupo de trabajo del artículo 29 recuerda que siempre ha opinado que la recopilación de datos masiva e indiscriminada no puede considerarse proporcionada en ningún caso[52].

3.3.3 Conclusión

A pesar de las limitaciones establecidas tras la introducción de la PPD-28, el Grupo de trabajo del artículo 29 mantiene su preocupación, especialmente en cuanto a la proporcionalidad de la recogida de datos. En primer lugar, existen indicios de que los EE. UU. siguen recopilando datos masivos e indiscriminados, o al menos no excluyen que todavía puedan hacerlo en el futuro. El Grupo de trabajo del artículo 29 ha declarado reiteradamente que esta recogida de datos no es conforme al Derecho de la UE y, por tanto, no es aceptable.

En segundo lugar, el Grupo de trabajo del artículo 29 señala que el tratamiento selectivo de datos o el tratamiento «lo más adaptado posible» también se pueden considerar masivos. La cuestión de si esta recogida de datos masivos debe permitirse o no es objeto actualmente de un procedimiento ante el TJUE. Por esta razón, el Grupo de trabajo del artículo 29 no realizará una evaluación final de la legalidad del tratamiento selectivo, pero masivo, de datos. No obstante, destaca que si el tratamiento selectivo, pero masivo, de datos se permitiese, los principios de segmentación se deberían aplicar tanto a la recogida como a la utilización posterior de los datos y no se podrían limitar únicamente a la utilización. En cualquier caso, es necesario aclarar el proyecto de Decisión de adecuación por lo que respecta a los seis propósitos mencionados en la PPD-28 para los que se pueden recoger datos «en bloque». En este momento, el Grupo de trabajo del artículo 29 no está convencido de que esos propósitos estén suficientemente restringidos para asegurar que la recogida de datos se limita ciertamente a lo necesario y proporcional.

3.4 Garantía C: Necesidad de que exista un mecanismo de supervisión independiente

Los EE. UU. no tienen un único organismo de supervisión a nivel federal encargado de las implicaciones de los programas de inteligencia y vigilancia para la privacidad y la protección de datos. En cambio, las actividades de inteligencia de los EE. UU. están sujetas a un procedimiento de supervisión a varios niveles y puede establecerse una distinción entre supervisión interna y supervisión externa. El Grupo de trabajo del artículo 29 reconoce que la práctica de información de los organismos de supervisión de los EE. UU. es muy detallada y, en su mayor parte, pública.

3.4.1 Supervisión interna

Todas las agencias de inteligencia y seguridad cuentan con personal responsable de garantizar el cumplimiento de sus respectivos marcos legislativos, incluidos inspectores generales cuya

[50] TJUE, asuntos acumulados C-203/15 y C-698/15.
[51] TJUE, asunto A-1/15.
[52] WP215, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf.

principal tarea es evaluar la conformidad global del trabajo de las agencias con la legislación, y en particular, aunque no exclusivamente, con la legislación relativa a la privacidad y la protección de datos. La existencia de inspectores generales está establecida por la ley y todos ellos son (o pronto lo serán) designados por el Presidente y confirmados por el Senado, en un intento de garantizar que estén organizados de manera independiente e informen al Congreso. Por tanto, el Grupo de trabajo del artículo 29 considera probable que los inspectores generales cumplan el criterio de independencia organizativa definido por el Tribunal de Justicia de la Unión Europea (TJUE) y el Tribunal Europeo de Derechos Humanos (TEDH), al menos a partir del momento en que el nuevo proceso de nombramiento se aplique a todos ellos. Por ahora persiste cierta preocupación suscitada por los inspectores generales que todavía son nombrados por el Director de la Agencia que supervisan.

Los inspectores generales pueden formular recomendaciones que pueden luego remitirse al Ministerio de Justicia y al PCLOB o incluso a la Comisión del Congreso que pueda ponerlas en práctica. Si un inspector general detecta una infracción, esta se puede abordar mediante medidas internas y políticas y se puede comunicar al Congreso. El inspector general es competente, por ejemplo, para llevar a cabo auditorías e inspecciones.

El Grupo de trabajo del artículo 29 señala que los informes del inspector general pueden ocultarse al público y que se puede impedir que un inspector general informe sobre si la información inspeccionada está clasificada. Sin embargo, los informes estarán en todo momento sujetos a la supervisión del Congreso, lo cual es una garantía fundamental, aun cuando no se ofrecen fundamentos jurídicos para interponer recursos individuales.

Todas las agencias tienen funcionarios de privacidad y libertades civiles que ayudan al sistema de autoinformación obligatoria con supervisión del Congreso.

En general, los mecanismos de supervisión interna en vigor pueden considerarse bastante sólidos; no obstante, para justificar una injerencia en los derechos fundamentales al respeto de la vida privada y a la protección de los datos, la supervisión debe ser completamente independiente. Y aunque el Grupo de trabajo del artículo 29 respeta y agradece la labor de los distintos agentes de la privacidad y las libertades civiles, no puede concluir que cumplan el nivel necesario de independencia para actuar como supervisores independientes.

3.4.2 Supervisión externa

La supervisión externa consta de diferentes mecanismos: la supervisión judicial prevista en los artículos 501 y 702, garantizada por el Tribunal FISA (en lo sucesivo, el FISC), la supervisión del Comité de Inteligencia del Congreso y la labor del PCLOB.

El Grupo de trabajo del artículo 29 recuerda que lo ideal sería, como también han señalado el TJUE y el TEDH, que la supervisión quedase en manos de un juez para garantizar la independencia y la imparcialidad del procedimiento. Hasta hace poco, el procedimiento del FISC era un procedimiento *ex parte*, sin que se brindase a los afectados la posibilidad de ser oídos o incluso de conocer la existencia del asunto. Aún en la actualidad, el procedimiento del

FISC sigue siendo *ex parte*, si bien, tras la adopción de la Ley de libertades de los EE. UU., se introdujeron en el FISC los *amici curiae*. Los *amici curiae* actúan de manera independiente, pero su función no es defender a personas concretas que puedan estar implicadas en el asunto.

La Ley de libertades de los EE. UU. creó un grupo de *amici curiae* para asesorar al FISC en casos importantes. El Tribunal ha seleccionado a cinco abogados que han obtenido la habilitación de seguridad apropiada y ofrecen asesoramiento técnico, asisten a las audiencias del FISC y presentan informes, además de discutir sobre el fondo de los asuntos desde la perspectiva de la intimidad y los derechos civiles. No obstante, estos solo actuarán en casos importantes o cuando surjan cuestiones jurídicas nuevas[53].

El artículo 215 está casi totalmente sujeto a la supervisión judicial *ex ante* (pero no *ex post*), dado que todos los programas que se basan en el artículo 215 para la recogida están sujetos a la aprobación del FISC. El informe del PCLOB especifica que «el artículo 702 difiere de este marco tradicional de vigilancia electrónica de la FISA tanto en las normas aplicadas como en la falta de determinaciones individualizadas realizadas por la FISC. Según la ley, el Fiscal General y el Director de la Inteligencia Nacional realizan las certificaciones anuales que autorizan la vigilancia de las personas no estadounidenses que, de acuerdo con estimaciones razonables, se considera que se encuentran fuera de los EE. UU. para adquirir información de inteligencia exterior, sin especificar al FISC qué personas no estadounidenses se seleccionarán. [...] Tampoco se exige que el Gobierno demuestre las causas razonables que inducen a creer que un objetivo del artículo 702 sea una potencia extranjera o un agente de una potencia extranjera, como exige la FISA tradicional»[54].

En el Congreso, los comités de inteligencia también desempeñan una tarea supervisora para la aprobación de las actividades de inteligencia, en particular mediante la votación del presupuesto. Los Comités de Inteligencia del Senado y la Cámara reciben informes clasificados sobre las actividades de inteligencia. El FG debe informar a estos comités cada seis meses sobre la vigilancia electrónica de la FISA. Sigue sin estar claro para el Grupo de trabajo del artículo 29 en qué medida están en condiciones de discutir sobre el tratamiento de los datos personales de las personas, especialmente de las no estadounidenses.

El PCLOB es una parte independiente del poder ejecutivo del Gobierno de los EE. UU. investida con dos facultades fundamentales: (1) revisar y analizar las acciones que el poder ejecutivo lleva a cabo para proteger la nación (EE. UU.) del terrorismo, velando por que la necesidad de estas acciones quede compensada por la necesidad de proteger la intimidad y las libertades civiles, y (2) velar por que las preocupaciones en materia de libertad reciban una consideración adecuada en el desarrollo y la aplicación de las leyes, reglamentaciones y políticas relacionadas con los esfuerzos que se realizan para proteger la nación del terrorismo. El Grupo de trabajo del artículo 29 constata que el PCLOB tiene poder para citar ante los tribunales y acceder a la información clasificada. En el desempeño de su función, también se ocupa de comprobar la eficacia de los programas. Su supervisión no es previa a los hechos,

[53] Ley de libertades, título IV: Reformas del Tribunal de Vigilancia de la inteligencia exterior, artículo 401. Nombramiento de *amici curiae*.
[54] Informe del PCLOB sobre el programa de vigilancia ejecutado en virtud del artículo 702 de la FISA, pp. 24 y 25.

sino posterior. El PCLOB ha demostrado sus facultades independientes al declarar su disconformidad con el Presidente de los EE. UU. en cuestiones jurídicas. En particular, consideró que el programa de metadatos telefónicos del artículo 215 no estaba legalmente autorizado y concluyó que no era eficaz, pues no había pruebas de ataques peligrosos. Además, le PCLOB realizó un estudio de un año de duración del programa del artículo 702 y consideró que era legal y estaba claramente autorizado por la ley y que el artículo 702 ha resultado muy eficaz en diferentes cuestiones, entre las que se incluye el terrorismo. Por último, actuó en lo relativo a la exigencia de transparencia y constató que diferentes hechos clasificados no debían estarlo. Se entiende que el PCLOB informará sobre la aplicación de la PPD-28 en un futuro próximo. A este respecto, considera que, para conservar información sobre un nacional extranjero, el mero hecho de que esa persona sea un nacional extranjero no es suficiente.

El Grupo de trabajo del artículo 29 señala por último que el EO12333 no prevé el control judicial, la supervisión ni los mecanismos de recurso de los programas de vigilancia que se ejecutan sobre su propia base.

3.4.3 Conclusión

El proyecto de Decisión de adecuación demuestra que en los EE. UU. se ha implantado un planteamiento de múltiples niveles de los mecanismos de supervisión, tanto internos como externos. Pese a que el funcionamiento de los mecanismos de supervisión puede resultar confuso, el Grupo de trabajo del artículo 29 considera que, por lo general, existen suficientes mecanismos de supervisión internos. Sin embargo, al Grupo de trabajo del artículo 29 le preocupa que la supervisión de los programas de vigilancia emprendidos sobre la base del EO12333 sea insuficiente.

El Grupo de trabajo del artículo 29 constata que solo se ha dado respuesta a sus anteriores críticas por la falta de carácter contradictorio de los procedimientos emprendidos ante el FISC en cierta medida mediante la introducción de los *amici curiae*, encargados de «promover la protección de la intimidad y las libertades civiles». No obstante, el FISC no prevé una supervisión judicial efectiva de la selección de las personas no estadounidenses. Por otra parte, persisten algunas dudas sobre la capacidad del FISC de evaluar de manera efectiva los procedimientos de selección y minimización, como también estableció el PCLOB[55].

Garantía D: Necesidad de que los particulares dispongan de una tutela judicial efectiva

3.5.1 Recursos judiciales

3.5.1.1 Requisito de legitimación

El sistema estadounidense relativo al recurso judicial incluye una limitación importante: la constitución de los EE. UU. exige que la persona pruebe la legitimación, es decir, los demandantes deben demostrar que han sufrido un perjuicio u otro daño directo y que ese daño

[55] Informe del PCLOB sobre el programa de vigilancia ejecutado en virtud del artículo 702 de la FISA, p. 11.

se puede reparar. A nivel federal, no se pueden emprender acciones por el simple hecho de que un individuo o un grupo estén descontentos con una actuación gubernamental o con una ley[56]. Tal requisito parece quedar privado de virtualidad por la falta de notificación a las personas sometidas a vigilancia incluso cuando las medidas ya han finalizado. El TJUE y el TEDH han declarado en reiteradas ocasiones que los justiciables deben poder tener acceso a vías de recurso administrativo o judicial. El TEDH ha confirmado en su resolución sobre el asunto Zakharov que, en virtud de la jurisprudencia, cualquier persona puede acudir a los tribunales si tiene un motivo legítimo para sospechar una injerencia en sus derechos fundamentales[57].

Además, los extranjeros que se encuentran fuera de los EE. UU. no gozan de una protección constitucional completa en los EE. UU., según la jurisprudencia del Tribunal Supremo de los EE. UU.[58]. Así ocurre, en particular, en relación con la Cuarta Enmienda, que protege a los estadounidenses, pero no a quienes no lo son, de inspecciones e incautaciones irrazonables, y de la que se deriva gran parte del derecho a la intimidad de los EE. UU. Los ciudadanos europeos y otras personas europeas que viven fuera de los EE. UU. quedan simplemente excluidos de la cobertura de la Cuarta Enmienda[59].

La aplicación limitada de la Ley de recurso judicial (tanto en términos de contenido, puesto que incluye la seguridad nacional, como en relación con las personas que pueden invocarla), las numerosas exenciones y la inseguridad jurídica en cuanto a las agencias a las que se aplicará la Ley de recurso judicial no cumplen el requisito de ofrecer un procedimiento efectivo de recurso a todas las personas afectadas en los casos de vigilancia de la inteligencia en relación con la seguridad nacional.

3.5.1.2 Directiva de Política Presidencial 28

El Grupo de trabajo del artículo 29 señala que la PPD-28 no es más que una Directiva y, por tanto, no puede crear derechos para los particulares. Esto solo puede hacerse a través de la legislación. Por lo tanto, los particulares no pueden acudir a los tribunales basándose en una presunta violación de las salvaguardias de la PPD-28.

3.5.1.3 Ley de vigilancia de la inteligencia exterior

En virtud de la FISA, existen algunas vías de recurso para las personas en caso de vigilancia ilícita. Con arreglo a la FISA, «una persona perjudicada que no sea una potencia extranjera o un agente de una potencia extranjera [...], respectivamente, que haya sido sometida a vigilancia electrónica o cuya información obtenida mediante vigilancia electrónica se haya divulgado o utilizado en contravención del artículo 1809 del presente título tendrá derecho a emprender acciones legales contra cualquier persona que haya cometido tal contravención». Sin embargo, quedan expresamente excluidos las potencias extranjeras y los agentes de

[56] https://www.law.cornell.edu/wex/standing; https://www.law.cornell.edu/wex/standinghttps://www.law.cornell.edu/wex/standing; Clapper/Amnesty International USA.
[57] TEDH, Zakharov, apartado 171.
[58] EE. UU./Verdugo - Urquidez , p. 264-266.
[59] Informe de los Copresidentes de la UE, sección 2.

potencias extranjeras que hayan sido objeto de la medida, y, como ya se ha señalado, el demandante tendrá que demostrar que dispone de legitimación, lo que no será posible en la práctica.

La Ley de libertades de EE. UU. ha creado un panel consultivo de *amici curiae* en el Tribunal de la FISA para dar asesoramiento (optativo) en caso de nuevas interpretaciones jurídicas importantes. En cualquier caso, la tarea de este panel consiste en proporcionar asesoramiento imparcial, y no en defender los intereses de una persona determinada a petición de esta.

3.5.2 Recursos administrativos

3.5.2.1 Inspectores generales

También existe la posibilidad de presentar una reclamación ante un inspector general. No obstante, los inspectores generales no tienen la obligación de examinar cada reclamación: no existe un derecho a ser oído, sino una facultad discrecional. El inspector general también puede publicar informes con las conclusiones de las infracciones cuando la información está desclasificada. Si un particular llega a suponer que el informe le afecta a él, tendrá la posibilidad de acudir a la justicia basándose en la constatación de la infracción.

3.5.2.2 Ley de libertad de información

Un recurso a disposición de todas las personas es la presentación de una solicitud de libertad de información, sobre la base de la Ley de libertad de información (FOIA). Según el Gobierno de los EE. UU., normalmente puede presentar esta solicitud cualquier persona (ciudadano estadounidense o no) simplemente pidiendo acceso a cualquier registro que obre en poder de una agencia. Esto incluye los registros sobre la persona, aunque en tal caso esta está obligada a facilitar un certificado de identidad. No obstante, si la información está clasificada para proteger la seguridad nacional, es poco probable que una solicitud FOIA prospere, pues se aplica una exención: las agencias no están obligadas a facilitar el acceso a información clasificada, ni siquiera si esa información se refiere a la persona que ha presentado la solicitud. La información procedente de investigaciones policiales en curso está totalmente excluida de las solicitudes FOIA. Por último, el Grupo de trabajo del artículo 29 entiende que la solicitud FOIA no da derecho a que una autoridad independiente compruebe la legalidad del tratamiento.

3.5.3 Defensor del Pueblo en el ámbito del Escudo de la privacidad

3.5.3.1 Creación de la figura del Defensor del Pueblo

El Escudo de la privacidad establece un nuevo mecanismo para que los «particulares de la UE» presenten solicitudes en relación con la «inteligencia de señales de los EE. UU.» al recién creado Defensor del Pueblo en el ámbito del Escudo de la privacidad. El cargo de Defensor del Pueblo, como se explica en el memorando adjunto a la carta del Secretario de Estado John Kerry de 22 de febrero de 2016, lo ocupará la Subsecretaria C. Novelli. La Subsecretaria Novelli desempeñará dicha función además de su papel de «coordinadora

principal para la diplomacia internacional sobre tecnología de la información», previsto en el artículo 4, letra d), de la PPD-28. En la carta y en el memorando se insiste en que la «Subsecretaria dependerá directamente ante el Secretario de Estado y es independiente de los servicios de inteligencia».

En el memorando se explica que, pese al nombre de su cargo, el Defensor del Pueblo en el ámbito del Escudo de la privacidad no solo tramitará las solicitudes relativas al acceso de la seguridad nacional a los datos transmitidos desde la UE a los EE. UU. de conformidad con el Escudo de la privacidad, sino también aquellas relativas a datos transmitidos en virtud de cláusulas contractuales normalizadas, normas empresariales vinculantes, excepciones (con arreglo al artículo 26 de la Directiva 95/46/CE) o «posibles excepciones futuras», tal como se definen en la nota a pie de página n.º 2 del memorando.

El modo en que se supone que funciona el mecanismo puede resumirse como sigue: un particular de la UE presenta una solicitud ante un organismo de un Estado miembro competente para la supervisión de los servicios de seguridad nacional, o a un «organismo de tramitación de reclamaciones de particulares de la UE» centralizado, en caso de que se designe o cree tal organismo. La autoridad que remite la solicitud a la institución del Defensor del Pueblo tendrá que comprobar en primer lugar si la solicitud está completa, tal como se define en el punto 3, letra b), de la carta[60]. Una vez recibida la solicitud por el Defensor del Pueblo en el ámbito del Escudo de la privacidad, este verificará que está completa de conformidad con la sección 3 b) y ofrecerá una respuesta, lo que significa que finalmente confirmará «i) que la reclamación ha sido debidamente investigada; y ii) la observancia de las leyes, estatutos, órdenes ejecutivas, directivas presidenciales y políticas de los organismos estadounidenses, siempre y cuando se hayan respetado las limitaciones y las protecciones descritas en la carta de la ODNI o, en caso de incumplimiento, cuando este incumplimiento haya sido subsanado»[61]. La respuesta «no confirmará ni negará si el individuo ha sido objeto de vigilancia ni tampoco confirmará la reparación concreta aplicada»[62]. En cuanto a la pregunta de cómo se lleva a cabo la investigación del Defensor del Pueblo, se explica que el Defensor del Pueblo en el ámbito del Escudo de la privacidad «colaborará estrechamente con otros funcionarios del Gobierno estadounidense, incluidos los organismos de vigilancia independientes»[63] y, más concretamente, «podrá coordinarse con la Office of the Director of

[60] b. El organismo de tramitación de las reclamaciones de ciudadanos de la UE garantizará, de conformidad con las siguientes acciones, que la solicitud esté completa:
i) Comprobará la identidad de la persona y que dicha persona actúe en su propio nombre y no como representante de una entidad gubernamental o intergubernamental.
ii) Comprobará que la solicitud sea por escrito y que contenga la siguiente información básica:
• cualquier información que constituya la base para la solicitud,
• la naturaleza de la información o de la reparación solicitada,
• las entidades del Gobierno de los Estados Unidos presuntamente implicadas, si las hay, y
• el resto de medidas adoptadas para obtener la información o la reparación solicitada y la respuesta recibida a través de esas otras medidas.
iii) Comprobará que la solicitud corresponda a unos datos que se acredite razonablemente que han sido transferidos desde la UE a los Estados Unidos en virtud del Escudo de la privacidad, las cláusulas contractuales estándar, las normas vinculantes para las empresas, las excepciones o las posibles futuras excepciones.
iv) Procederá a una determinación inicial de que la solicitud no sea infundada, abusiva o presentada de mala fe.
[61] Escudo de la privacidad, anexo III, apartado 4.e.
[62] Escudo de la privacidad, anexo III, apartado 4.e.
[63] Escudo de la privacidad, anexo III, apartado 2.a.

National Intelligence (Oficina del Director de Inteligencia Nacional), el Departamento de Justicia y otros departamentos y organismos implicados en la seguridad nacional de los EE. UU., y con los inspectores generales, los agentes responsables de la ejecución de la Freedom of Information Act (Ley relativa a la libertad de información) y los agentes responsables de la protección de las libertades civiles y la privacidad»[64]. Esta coordinación deberá ser tal que garantice que el Defensor del Pueblo en el ámbito del Escudo de la privacidad pueda enviar una respuesta en la que se incluyan las confirmaciones según lo descrito anteriormente.

3.5.3.2 Evaluación del nuevo mecanismo del Defensor del Pueblo

El Grupo reconoce los esfuerzos realizados por la Comisión Europea y el Gobierno estadounidense para introducir un nuevo mecanismo con vistas a mejorar las posibilidades de reparación por vía judicial en relación con las actividades de vigilancia de los EE. UU. Entiende que la evaluación de este mecanismo, en cuanto que novedad en las relaciones internacionales sobre inteligencia de señales o seguridad nacional, reviste particular importancia.

En esta sección, el Grupo de trabajo del artículo 29 evaluará la relación existente entre la creación de la figura del Defensor del Pueblo en el ámbito del Escudo de la privacidad con los requisitos necesarios para que las personas puedan obtener una reparación por vía judicial, tal como se recoge en la Carta, el CEDH y la jurisprudencia de los tribunales europeos.

3.5.3.3 ¿Puede ser suficiente per se *la creación de la figura del Defensor del Pueblo?*

Para empezar, cabe preguntarse si la creación de la figura del «defensor del pueblo» puede considerarse conforme con el artículo 47 de la Carta, que hace referencia a un recurso efectivo ante un tribunal imparcial[65], al menos si no hay ninguna otra vía disponible para obtener una reparación por vía judicial. Esto es importante, ya que el TJUE se refiere en Schrems, en su importante consideración 95, al artículo 47 de la Carta, y ello sin dar ninguna indicación de que el artículo 47 deba entenderse con modificaciones en el contexto de las medidas de vigilancia. Sin embargo, en el asunto Kadi II[66] el TJUE ya aplicó el artículo 47 de la Carta a medidas de vigilancia de la seguridad nacional e internacional[67].

En cualquier caso, la jurisprudencia del TEDH explica muy claramente que la reparación por vía judicial ante los tribunales ordinarios no es una condición para considerar que los sistemas de vigilancia son conformes con el artículo 8 (y con el artículo 13 del CEDH)[68]. Por el

[64] Escudo de la privacidad, anexo III, apartado 2.a.
[65] Por otra parte, en las explicaciones sobre la Carta de los Derechos Fundamentales ha quedado establecido que el artículo 47 debe interpretarse en el sentido de ofrecer una garantía del derecho a la tutela judicial efectiva ante un órgano jurisdiccional [explicaciones relativas a la Carta de los derechos fundamentales, explicación relativa al artículo 47 (2007/C 303/02)].
[66] Asuntos acumulados C-584/10 P, C-593/10 P y C-595/10 P, Comisión Europea y Reino Unido/Kadi, 18 de julio de 2013.
[67] Sentencia Kadi II, apartados 97 y 100: todos los actos de la Unión, incluidos los que están destinados a aplicar resoluciones aprobadas por el Consejo de Seguridad en virtud del capítulo VII de la Carta de las Naciones Unidas, están sometidos al control de la legalidad efectuado por los órganos jurisdiccionales de la Unión Europea (el capítulo VII trata de la actuación en caso de amenazas a la paz, quebrantamientos de la paz o actos de agresión).
[68] El artículo 13 del CEDH obliga a los Estados miembros a velar por que toda persona cuyos derechos y libertades hayan sido violados tenga derecho «a la concesión de un recurso efectivo ante una instancia nacional». No tiene que tratarse necesariamente de una autoridad judicial, como ha aclarado el TEDH en Klass, apartados 56 y 67.

contrario, el Tribunal ha establecido en virtud del artículo 8, como protección necesaria ante las actividades de vigilancia, que un recurso ante otras autoridades puede ser procedente. El TEDH tiene, no obstante, grandes esperanzas en que otras autoridades proporcionen una tutela judicial efectiva, y afirma que tal autoridad debe ser independiente de las autoridades que encargadas de la vigilancia y están investidas de poderes y atribuciones suficientes para ejercer un control eficaz y permanente[69].

En los asuntos Kennedy y Klass, el TEDH dio una indicación de lo que estas expectativas podían significar en el contexto de la vigilancia secreta, cuando el interesado no está informado del tratamiento de sus datos. En ambas sentencias el TEDH consideró que las autoridades eran independientes, y especialmente independientes de los organismos encargados de la vigilancia, pero también de las instrucciones[70] de cualquier otra autoridad. Más concretamente, en el asunto Kennedy el Tribunal aprobó una autoridad independiente e imparcial que había adoptado su propio reglamento interno y estaba formada por miembros que ostentaban o habían ostentado altos cargos judiciales y abogados especializados[71].

En el marco de su examen de las reclamaciones presentadas por particulares, las autoridades de ambas sentencias tuvieron acceso a toda la información pertinente, incluidos los materiales clasificados. Por último, ambas tenían facultades para corregir el incumplimiento[72].

Además de plantear la cuestión de si el Defensor del Pueblo se puede considerar un «tribunal», la aplicación del artículo 47, apartado 2, de la Carta plantea otro reto, pues establece que el tribunal ha de estar «establecido por ley». Cabe preguntarse, sin embargo, si un memorando en el que se detalla el funcionamiento de un nuevo mecanismo puede considerarse «ley».

Por consiguiente, teniendo en cuenta el principio de equivalencia sustancial, en lugar de evaluar si un Defensor del Pueblo puede considerarse formalmente un tribunal establecido por ley, el Grupo de trabajo decidió trabajar más a fondo los matices de la jurisprudencia por lo que se refiere a los requisitos específicos necesarios para considerar que los «recursos jurídicos» y la «reparación por vía judicial» son conformes con los derechos fundamentales de los artículos 7, 8 y 47 de la Carta y con el artículo 8 (y el 13) del CEDH. En su análisis ulterior, al debatir el ámbito de aplicación del nuevo mecanismo, el Grupo de trabajo se centrará, pues, en los siguientes criterios: el requisito de presentar una solicitud a la institución del Defensor del Pueblo y de recibir una respuesta (en lo sucesivo, «legitimación»), la independencia del Defensor del Pueblo, sus facultades de investigación para acceder al material necesario, incluidos los documentos clasificados, y de solicitar la asistencia de otros organismos, y, por último, su facultad para corregir el incumplimiento.

[69] Klass, apartados 56 y 67.
[70] TEDH, Klass, apartados 21 y 53.
[71] La Comisión G 10 (en el momento de la sentencia) estaba compuesta por tres miembros, de los cuales el Presidente debe estar cualificado para ejercer una función judicial (Klass, apartados 21 y 53).
[72] TEDH, Kennedy, apartado 167; Klass, apartados 21 y 53.

3.5.3.4 Ámbito de aplicación del mecanismo del Defensor del Pueblo

Por lo que se refiere al acceso al mecanismo del Defensor del Pueblo, el Grupo de trabajo del artículo 29 considera que todos aquellos que estén sujetos a la legislación de la UE deberían quedar cubiertos por las salvaguardias del Escudo de la privacidad. No sería aceptable establecer una distinción basada en la nacionalidad, ya que los derechos fundamentales de la UE se aplican a todas las personas, y no solo a los titulares de un pasaporte de la UE. El anexo III se refiere a una «persona de la UE» sin definir quiénes pueden considerarse como tales. El Grupo de trabajo lamenta esta incertidumbre y sugiere que se prevea una aclaración en el sentido de que todas las personas sujetas a la legislación de la UE tienen derecho a que su petición al Defensor del Pueblo se tramite de acuerdo con las condiciones del memorando. Además, la Comisión y los EE. UU. deben abordar la cuestión de en qué medida el Escudo de la privacidad también se aplicará a los ciudadanos y residentes de los países del EEE y Suiza, que en el pasado quedaban cubiertos por el régimen de puerto seguro.

Por otra parte, el Grupo de trabajo del artículo 29 constata cierta incertidumbre en cuanto al alcance de la aplicación del mecanismo del Defensor del Pueblo. Aunque el memorando establece que el Defensor del Pueblo se encarga de tramitar las solicitudes relativas a la seguridad nacional de los datos transmitidos desde la UE a los EE. UU. de conformidad con todos los instrumentos de transferencia disponibles en virtud del Derecho de la UE, también deja igualmente claro que establece un mecanismo «en relación con la inteligencia de señales». Este último concepto sugiere que solo dichas transferencias de datos están cubiertas en caso de que los datos se recojan por medio de inteligencia de señales, lo que plantea la cuestión de si los datos recogidos en virtud de la FISA, por ejemplo, se consideran «inteligencia de señales». Tal parece ser el caso por lo que respecta al artículo 702, según se explica en la observación de la ODNI, p. 10[73]. Sin embargo, el Grupo de trabajo del artículo 29 lamenta que el uso de la expresión «inteligencia de señales» genere una incertidumbre innecesaria en este contexto.

Otra consecuencia es que el Grupo de trabajo entiende que el mecanismo del Defensor del Pueblo no cubre las solicitudes relacionadas con el acceso por parte de los organismos de seguridad[74]. Si así fuera, no quedaría claro si las solicitudes de algunas agencias, y en particular las de la CIA, quedarían cubiertas por el mecanismo.

3.5.3.5 «Legitimación» y procedimiento de solicitud

Emprender acciones judiciales contra las medidas de vigilancia del Gobierno de los EE. UU. ante los tribunales estadounidenses ordinarios es muy difícil. El Grupo de Trabajo es consciente de que el Tribunal Supremo ha denegado la legitimación en los casos de datos de inteligencia en los que el solicitante no pudo demostrar «perjuicio concreto, particularizado, real o inminente»[75]. En este sentido, la creación de la institución del Defensor del Pueblo constituye un paso importante, pues añade una posibilidad de reparación por vía judicial que

[73] Escudo de la privacidad, anexo VI, p. 10.
[74] Memorando sobre la creación de un Defensor del Pueblo, p. 1.
[75] Clapper/Amnesty International USA, 568 U.S. (2013) II. p.10.

de otro modo no existiría. Por lo tanto, el Grupo de trabajo acoge con satisfacción la aclaración que figura en la sección 3(c). Basándose en esa sección, para presentar una solicitud con arreglo al nuevo mecanismo no es necesario demostrar que se ha accedido realmente a los datos del solicitante por medio de actividades de inteligencia de señales.

El Grupo de Trabajo aprueba ampliamente el procedimiento de identificación del demandante en el marco del mecanismo del Defensor del Pueblo. Es lógico hacer que la identificación tenga lugar en territorio de la UE, y lo mismo sucede con el mecanismo de acceso al amparo del Acuerdo TFTP 2 UE-EE. UU. Sin embargo, el Grupo de Trabajo considera incomprensible que la verificación de la UE deba ser llevada a cabo por «organismos de los Estados miembros competentes para la supervisión de los servicios de seguridad nacional». Para empezar, parece improbable que a resultas del artículo 4, apartado 2, del Tratado de la Unión Europea, la Comisión Europea esté en condiciones de encomendar tareas a esos organismos que son claramente competencia de los Estados miembros.

Además, dada la diversidad de los mecanismos de supervisión de los servicios de seguridad nacional de los Estados miembros, la participación de las autoridades correspondientes podría afectar seriamente a la eficacia del sistema ante los ciudadanos de los Estados miembros. Por ejemplo, en los casos en que existan varias autoridades encargadas de la supervisión de los servicios de seguridad nacional y pueda resultar difícil para el particular determinar cuál es la pertinente, cuando el régimen jurídico nacional aplicable no prevea la posibilidad de que los particulares se pongan en contacto con el organismo de supervisión pertinente o cuando dichas autoridades no estén establecidas de forma que sean aptas para desempeñar las tareas que se les hayan impuesto en el proyecto de Decisión de adecuación[76]. Teniendo en cuenta la participación de las APD en la aplicación y la supervisión del Escudo de la privacidad, así como su papel similar en el marco del Acuerdo TFTP2, es más lógico atribuir esta tarea a las autoridades nacionales de protección de datos de los Estados miembros. El Grupo de Trabajo subraya que considera improbable que la información clasificada se trate como parte de un procedimiento ante el Defensor del Pueblo en el ámbito del Escudo de la privacidad, puesto que la respuesta siempre será «conforme o no conforme, pero corregido».

3.5.3.6 Independencia

Las declaraciones del Secretario de Estado ponen de manifiesto que el cargo de Defensor del Pueblo lo ocupará un Subsecretario del Departamento de Estado. El nombramiento lo realiza el Presidente y precisa la confirmación del Senado. La función del Defensor del Pueblo no requiere confirmación adicional, la atribución de la función del Defensor del Pueblo es suficiente. El Subsecretario es designado por el Presidente de los EE. UU., dirigido por el Secretario de Estado como Defensor del Pueblo y confirmado por el Senado estadounidense en el ejercicio de su cargo de Subsecretario. Como se destaca en las declaraciones de la carta y el memorando, el Defensor del Pueblo «es independiente de los servicios de inteligencia de los EE. UU.». No obstante, el Grupo de trabajo del artículo 29 cuestiona si la institución del Defensor del Pueblo se ha creado en el departamento más adecuado. Para cumplir con

[76] Por ejemplo, en algunos Estados miembros de la UE, los particulares solo pueden acceder a la información en poder de los servicios de seguridad nacional a través de una petición de un juez del Tribunal Superior de Justicia.

eficacia la función de Defensor del Pueblo parece necesario conocer y comprender el funcionamiento de los servicios de inteligencia, pero para poder actuar con independencia se precisa, al mismo tiempo, cierta distancia de los servicios de inteligencia.

El Escudo de la privacidad no establece criterios específicos para la destitución del Defensor del Pueblo. Por lo tanto, el Grupo de trabajo entiende que el Defensor del Pueblo puede ser destituido de su cargo de Defensor del Pueblo de la misma manera que puede ser destituido de su cargo de Subsecretario del Departamento de Estado, lo cual puede llegar a menoscabar la independencia del Defensor del Pueblo.

A primera vista, designar a un Subsecretario del Departamento de Estado como Defensor del Pueblo es claramente diferente, en términos de independencia, de atribuir competencias a un tribunal ordinario para ofrecer reparación por vía judicial a las personas. Por tanto, la cuestión es si el Defensor del Pueblo se puede considerar, en términos de independencia, igual a otros organismos de supervisión independientes que han resultado independientes de manera efectiva. En el contexto de la vigilancia, estos podrían ser, en particular, el Tribunal de poderes de investigación (IPT) del Reino Unido y en la Comisión G10 en Alemania.

Para analizar si tal es el caso, es preciso además que al realizar la evaluación se analicen las facultades otorgadas a los «independientes».

3.5.3.7 Competencias de investigación

En el asunto Kadi II, el TJUE dictaminó, en relación con el artículo 47 de la Carta, que «el interesado pueda conocer los motivos de la resolución adoptada con respecto a él, bien mediante la lectura de la propia resolución, bien mediante la notificación de la motivación de ésta efectuada a petición suya, sin perjuicio de la facultad del juez competente de exigir a la autoridad de que se trate que comunique tal motivación, a fin de permitir que el interesado defienda sus derechos en las mejores condiciones posibles»[77]. Los tribunales de la Unión Europea se deben asegurar de que la decisión dispone de unos fundamentos de hecho suficientemente sólidos[78]. Este establece claramente que «no cabe oponer el secreto o la confidencialidad», al menos ante los órganos jurisdiccionales de la Unión Europea[79]. Por lo tanto el Grupo de trabajo concluye que, para cumplir los requisitos del TJUE[80], el Defensor del Pueblo debe disponer de información y pruebas que respalden los motivos invocados para llevar a cabo una medida.

Todavía no está claro qué alcance tendrían las competencias de investigación del Defensor del Pueblo. Ni el proyecto de Decisión de la Comisión ni el anexo III del Departamento de Estado son excesivamente claros a este respecto. Según entiende el Grupo de trabajo, el Defensor del Pueblo debe recibir información suficiente para poder indicar si una operación de tratamiento de datos por los servicios de seguridad se lleva a cabo de conformidad con la ley y, si no es

[77] Sentencia Kadi II, apartado 100.
[78] Sentencia Kadi II, apartado 119.
[79] Sentencia Kadi II, apartado 125.
[80] Sentencia Kadi II, apartado 122; aunque la autoridad de que se trate no ha de presentar todos los datos y pruebas inherentes a los motivos de la medida.

así, para asegurarse de que se corrija la situación de incumplimiento. Ahora bien, ni la carta del Departamento de Estado ni el proyecto de Decisión de la Comisión precisan si el Defensor del Pueblo tendría acceso directo a la información de la persona de que se trate y, por tanto, puede llevar a cabo su propia investigación, o si solo puede referirse a los informes de otros funcionarios del Gobierno de los EE. UU.

3.5.3.8 Competencias de corrección

Sigue sin estar claro en el memorando cómo puede el Defensor del Pueblo ordenar que se subsane un incumplimiento. A la falta de claridad en lo relativo a las competencias de investigación, se suman las dudas sobre la medida en que el Defensor del Pueblo como tal será efectivamente capaz de ordenar que se subsane el incumplimiento y cuál ha de ser el resultado de tal ejercicio. ¿Significaría esto que los datos obtenidos de un modo no conforme (ilegalmente) ya no pueden utilizarse en ningún procedimiento y deben suprimirse?

Además, el Grupo de trabajo entiende que el Escudo de la privacidad no prevé ningún procedimiento de recurso o revisión contra la «decisión» del Defensor del Pueblo.

Por último, en lo que se refiere a la comunicación del Defensor del Pueblo al demandante tras el examen de una reclamación, el Defensor del Pueblo no deberá indicar si se ha producido algún comportamiento ilegal de los servicios de inteligencia. La respuesta será siempre la misma y será vaga. En el asunto Kadi II, el TJUE dictaminó que la autoridad competente (como organismo de supervisión) tiene la obligación de exponer los motivos en cualquier circunstancia, si bien el artículo 296 del TFUE no exige una respuesta detallada[81].

3.5.4 Conclusión

La existencia de una tutela judicial efectiva para las personas sigue siendo motivo de preocupación para el Grupo de trabajo del artículo 29. En primer lugar, el proyecto de Decisión de adecuación no proporciona una respuesta clara a la pregunta de en qué situaciones y en qué condiciones previas los particulares pueden interponer un recurso con el fin de determinar sus derechos.

El Grupo de trabajo del artículo 29 reconoce y valora positivamente la introducción de un mecanismo de recurso alternativo en forma de Defensor del Pueblo, lo que constituye un acontecimiento único en las relaciones entre la UE y un tercer país. Además de la necesidad de clarificar el concepto de «ciudadanos de la UE», tal como se ha planteado antes, el mecanismo crea una vía adicional para obtener reparación ante la administración de los EE. UU. con el fin de garantizar que todos los datos personales del demandante se traten de conformidad con la legislación estadounidense.

Al mismo tiempo, al evaluar el mecanismo del Defensor del Pueblo teniendo en cuenta las normas aplicables a un tribunal independiente en el sentido del artículo 47 de la Carta y los requisitos que el TJUE y TEDH han establecido en sus jurisprudencias en los asuntos de

[81] Sentencia Kadi II, apartado 116.

vigilancia, el Grupo de trabajo del artículo 29 detecta deficiencias significativas. En primer lugar, existe cierta preocupación en cuanto a si el Defensor del Pueblo puede considerarse (formal y plenamente) independiente, en especial debido a la relativa facilidad con que los responsables políticos pueden ser destituidos. En segundo lugar, persisten las preocupaciones relativas a las facultades del Defensor del Pueblo para ejercer un control efectivo y continuo. Sobre la base de la información disponible en el anexo III, el Grupo de trabajo del artículo 29 no puede llegar a la conclusión de que el Defensor del Pueblo pueda tener en todo momento acceso directo a toda la información, los ficheros y los sistemas de TI necesarios para hacer su propia evaluación, ni que realmente pueda obligar a las agencias de inteligencia responsables a poner fin a todo tratamiento de datos no conforme, sobre todo en caso de desacuerdo sobre la cuestión de si el tratamiento de datos se ajusta a la ley o no. Posiblemente, una mayor clarificación del lugar que ocupa el Defensor del Pueblo y de sus facultades disiparía las dudas del Grupo de trabajo del artículo 29.

3.6 Observaciones finales sobre las protecciones y limitaciones aplicables a las autoridades de seguridad nacional de los EE. UU.

En primer lugar, el Grupo de trabajo del artículo 29 felicita a la Comisión y a las autoridades estadounidenses por todos los esfuerzos que han realizado para aumentar la transparencia del efecto que los programas de vigilancia estadounidenses puedan tener en los datos transferidos de conformidad con el Escudo de la privacidad (o cualquier otro instrumento de transferencia de datos). Se han tomado medidas significativas desde las primeras revelaciones de Snowden, en junio de 2013. Sin embargo, el Grupo de trabajo del artículo 29 indica que siguen existiendo motivos de preocupación. Cuando menos, se necesitan explicaciones y aclaraciones adicionales sobre los derechos y obligaciones en el marco del Escudo de la privacidad.

Las dos preocupaciones principales del Grupo de trabajo del artículo 29 son que las autoridades estadounidenses no excluyan completamente la recogida masiva e indiscriminada de datos y que las competencias y el cargo del Defensor del Pueblo no se hayan explicado con mayor detalle. Por otra parte, las APD nacionales deberían ser competentes para incoar un procedimiento ante el Defensor del Pueblo en nombre de una persona, en lugar de los organismos de supervisión de las agencias de inteligencia. Además, aunque el Grupo de trabajo del artículo 29 reconoce ciertamente el intento de responder a las preocupaciones planteadas por las APD, sería de agradecer que se adoptasen nuevas salvaguardias para garantizar que las injerencias que puedan causar los programas de vigilancia de los EE. UU. son necesarias en una sociedad democrática.

4. EVALUACIÓN DE LAS GARANTÍAS DE LA APLICACIÓN DE LA LEY DEL ESCUDO DE LA PRIVACIDAD

4.1 Introducción

En lo que respecta al acceso público a los datos personales a efectos de aplicación de la legalidad, el Grupo de trabajo del artículo 29 señala que los principios de privacidad del

anexo II del Escudo de la privacidad contienen una excepción idéntica a la establecida en los principios de puerto seguro. Por consiguiente, el carácter general de la excepción se ha mantenido, lo que significa que los nuevos principios del Escudo de la privacidad permitirán injerencias en los derechos fundamentales de las personas cuyos datos personales se transfieren desde la UE a los EE. UU. «fundadas en exigencias concernientes a la seguridad nacional, el interés público y el cumplimiento de la ley de Estados Unidos»[82].

Sin embargo, una de las principales críticas expresadas por el Tribunal en relación con la Decisión de puerto seguro en Schrems fue que no contenía «ninguna constatación sobre la existencia en EE. UU. de reglas estatales destinadas a limitar las posibles injerencias en los derechos fundamentales de las personas cuyos datos se transfieran desde la Unión a Estados Unidos».

Así pues, el Grupo de trabajo del artículo 29 acoge con satisfacción los esfuerzos de la Administración estadounidense para ofrecer una visión más precisa del marco jurídico relativo a la injerencia en los datos personales transferidos en el marco del Escudo de la privacidad a efectos de aplicación de la ley, incluidas las limitaciones y salvaguardias aplicables. Al mismo tiempo, el Grupo de trabajo del artículo 29 hace hincapié en que considera la cuestión del acceso del público teniendo en cuenta que cualquier injerencia en los derechos fundamentales a la vida privada y a la protección de datos debe estar justificada en una sociedad democrática. Por consiguiente, el Grupo de trabajo del artículo 29 ha analizado las garantías de aplicación de la ley del Escudo de la privacidad, utilizando el marco establecido en la sección 1.2 del presente dictamen.

4.2 Aplicación de las garantías esenciales europeas al acceso por parte de las fuerzas y cuerpos de seguridad a datos que obren en poder de las empresas

4.2.1 El acceso de las fuerzas y cuerpos de seguridad a los datos personales debe ser conforme a la ley y basarse en normas claras, precisas y accesibles

El anexo VII del Escudo de la privacidad contiene una carta del Departamento de Justicia de los EE. UU. que «ofrece una breve visión general de las principales herramientas de investigación utilizadas para la obtención de datos comerciales y otra información de registros de empresas en los EE. UU. a efectos de la aplicación del Derecho penal o en aras del interés público (civil y reglamentario), incluidas las limitaciones de acceso que acompañan a estas competencias».

Todos los procedimientos mencionados en el anexo VII se derivan directamente de la Constitución (la Cuarta Enmienda), del derecho común y procesal o de directrices y políticas del Departamento de Justicia de los EE. UU. No obstante, el anexo VII no se refiere específicamente a todas las leyes que prevén estos procedimientos, sino que se centra en describir los procedimientos brevemente. El anexo VII indica igualmente que «existen otras bases jurídicas para que las sociedades puedan impugnar las solicitudes de datos de los órganos administrativos en función sectores concretos y de los tipos de datos que posean», y

[82] Schrems, apartado 87.

da varios ejemplos no exhaustivos, tales como la Ley de Secreto Bancario, la Ley sobre Informes de Crédito Justos y el Derecho a la Ley de Privacidad Financiera.

El Grupo de trabajo del artículo 29 observa que el marco de las leyes, procedimientos y políticas está fragmentado, y que la base jurídica aplicable a una determinada solicitud de acceso dependerá de la naturaleza de los datos recabados, la naturaleza de la empresa, la naturaleza de los procedimientos legales (penales, administrativas, relativos a otros ámbitos de interés público) y la naturaleza de la entidad que solicita el acceso.

Dado que todas las normas aplicables para limitar el acceso de las fuerzas y cuerpos de seguridad a los datos transferidos de conformidad con el Escudo de la privacidad se basan en la Constitución, en el Derecho común y en políticas transparentes del Departamento de Justicia, el Grupo de trabajo del artículo 29 tiene en cuenta una presunción de accesibilidad de estas normas. No obstante, el grado de claridad y de precisión de las normas solo puede evaluarse en cada tipo de procedimiento y solicitud de acceso. Por consiguiente, el Grupo de trabajo del artículo 29 lamenta señalar que, sobre la base de los datos disponibles en el anexo VII del Escudo de la privacidad y las conclusiones que figuran en el proyecto de Decisión, tal apreciación no puede efectuarse en este momento.

4.2.2 Se han de demostrar la necesidad y la proporcionalidad en relación con los objetivos legítimos perseguidos

El Grupo de trabajo del artículo 29 toma debida nota de que puede considerarse que la solicitud de acceso a datos con fines de aplicación de la ley persigue un objetivo legítimo. Por ejemplo, el artículo 8, apartado 2, del TEDH acepta las injerencias en el derecho a la protección de la vida privada por una autoridad pública cuando «sea necesaria para [...] la seguridad pública, [...] la defensa del orden y la prevención de las infracciones penales». Sin embargo, tales injerencias solo son aceptables cuando son necesarias y proporcionadas[83].

Según jurisprudencia reiterada del TJUE, el principio de proporcionalidad exige que las medidas legislativas que proponen injerencias en los derechos a la vida privada y a la protección de los datos personales sean adecuadas «para lograr los objetivos legítimos perseguidos por *la normativa de que se trate* y no rebasen los límites de lo que resulta apropiado y necesario para el logro de dichos objetivos»[84] (sin cursiva en el original). Por lo tanto, la evaluación de la necesidad y la proporcionalidad tiene lugar siempre en relación con una medida específica prevista por la legislación.

Las autoridades estadounidenses especifican en el anexo VII que los fiscales federales y los agentes de investigación federales podrán acceder a los documentos y otra información de registros de entidades «utilizando varios tipos de procesos jurídicos vinculantes, entre ellos citaciones para comparecer ante un gran jurado, citaciones administrativas y órdenes de investigación», y podrán obtener otras comunicaciones «gracias a las competencias penales

[83] Véase el documento de trabajo sobre las garantías esenciales, pp. 7-9. Para una evaluación general de los conceptos de necesidad y proporcionalidad, véase WP29, «Dictamen 01/2014 sobre la aplicación de los conceptos de necesidad y proporcionalidad y la protección de datos en el sector de los organismos con funciones coercitivas», 27 de febrero de 2014.
[84] Digital Rights Ireland, apartado 46 y jurisprudencia citada.

federales relativas al registro de llamadas y las escuchas telefónicas»[85]. Además, los organismos con responsabilidades civiles y reglamentarias podrán expedir requerimientos a las sociedades para la obtención de «registros comerciales, información almacenada electrónicamente u otros elementos tangibles»[86]. Por otra parte, el anexo VII especifica que estos procedimientos judiciales se utilizan en general para obtener información de «empresas» estadounidenses, independientemente de que si están certificadas o no en el marco del Escudo de la privacidad y «de la nacionalidad del interesado». En otras palabras, parece que los beneficiarias de estas protecciones son las sociedades, y no los particulares.

Además del anexo VII, el proyecto de Decisión, que se basa en los principios del Escudo de la privacidad, recoge las conclusiones de la Comisión en cuanto a la existencia en EE. UU. de normas para limitar las injerencias en los derechos fundamentales de las personas cuyos datos personales se transfieren desde la UE a los EE. UU. en el marco del Escudo de la privacidad.

En particular, las conclusiones del proyecto de Decisión hacen referencia a las limitaciones y salvaguardias aplicables previstas en la Cuarta Enmienda de la Constitución de los EE. UU., según las cuales los registros e incautaciones por parte de las fuerzas y cuerpos de seguridad requieren un mandamiento judicial por indicios razonables[87]. Las conclusiones también se refieren al hecho de que, en los casos excepcionales en que el requisito de la orden no se aplique, la aplicación de la ley estará sujeta a una prueba de razonabilidad[88].

No obstante, de las conclusiones no se desprende de qué manera se aplican estas salvaguardias a las personas no estadounidenses. De hecho, el proyecto de Decisión reconoce en un considerando que «la protección en virtud de la Cuarta Enmienda no se extiende a las personas no estadounidenses que no residen en los Estados Unidos»[89]. Asimismo, se indica en los mismos apartados del proyecto de Decisión que las personas no estadounidenses «se benefician indirectamente a través de la protección otorgada a las empresas de los EE. UU. en posesión de los datos personales y que son destinatarias de las solicitudes de intervención legal». El Grupo de trabajo del artículo 29 lamenta, sin embargo, que esta constatación no incluya ninguna referencia a una fuente jurídica, ya sea de Derecho común o de la jurisprudencia.

En conclusión, el Grupo de trabajo del artículo 29 señala que el sistema de herramientas de investigación utilizadas para obtener los datos comerciales y demás información de registro de las sociedades de los EE. UU. con fines de aplicación del Derecho penal o fines de interés público, incluidas las limitaciones de acceso y salvaguardias, constituye un entorno de medidas complejo. Sobre la base de la información disponible, este sistema no se puede evaluarse en términos generales en este momento. Se necesita una valoración específica de los casos concretos para evaluar certeramente la necesidad y la proporcionalidad de las medidas de investigación policial en relación con los derechos fundamentales a la vida privada y a la protección de datos.

[85] Anexo VII, p. 2.
[86] Anexo VII, p. 4.
[87] Proyecto de Decisión de adecuación, apartado 107.
[88] Escudo de la privacidad, apartado 107.
[89] Proyecto de Decisión de adecuación, apartado 108.

4.2.3 Debería existir un mecanismo de supervisión independiente

El Grupo de trabajo del artículo 29 señala debidamente que la mayoría de los procedimientos descritos en el anexo VII presuponen que se haya dictado de una decisión judicial antes de que las autoridades tengan acceso a los datos [por ejemplo, órdenes judiciales de identificación y registro de llamadas salientes *(pen registers)* o entrantes *(trap and trace devices)*, órdenes judiciales de vigilancia con arreglo a la Ley federal de escuchas, órdenes de registro; artículo 41]. No obstante, parece que no todos ellos exigen la intervención previa de un tribunal. Por ejemplo, las autoridades civiles y reguladoras «podrán expedir requerimientos»[90]. En estos casos, existe la posibilidad de un control judicial *ex post* de la razonabilidad del requerimiento, pues «el destinatario de un requerimiento administrativo podrá impugnar la aplicación de un requerimiento ante el tribunal»[91].

Sobre la base de la información disponible, el Grupo de trabajo del artículo 29 constata que, por lo que se refiere al acceso de las autoridades policiales a los datos que obren en poder de empresas de los EE. UU., parece que existe un mecanismo de supervisión independiente bastante sólido.

4.2.4 Debe haber una tutela judicial efectiva disponible para el interesado

Como ya se ha mencionado, «la protección en virtud de la Cuarta Enmienda no se extiende a las personas no estadounidenses que no residen en los Estados Unidos»[92]. Esto significa que una persona no estadounidense no estaría en condiciones de impugnar las órdenes o los requerimientos en el Tribunal invocando la Cuarta Enmienda. El proyecto de Decisión de adecuación especifica que las personas no estadounidenses se benefician indirectamente a través de la protección otorgada a las empresas de los EE. UU. en posesión de los datos personales y que son los destinatarios de las solicitudes de intervención legal. El Grupo de trabajo del artículo 29 observa no obstante que, aun cuando esta protección fuera eficaz, ello no significaría que existiera una tutela judicial efectiva disponible para las personas, ya que el objeto del derecho a la tutela judicial efectiva en este escenario parece ser la empresa que recibe la solicitud de acceso, y no la persona cuyos datos son objeto de controversia.

El anexo VII no contiene más información sobre posibles soluciones derivadas del Derecho común que estén a disposición de las personas no estadounidenses cuando las autoridades o las empresas proporcionen u obtengan ilegalmente acceso al contenido de sus datos.

El Grupo de trabajo del artículo 29 acoge con satisfacción que la recientemente adoptada Ley de recurso judicial[93] prevea derechos de recurso judicial para las personas no estadounidenses. Estos derechos se limitan, no obstante, a motivos de recurso bien definidos: el derecho de rectificación y acceso a los datos y los honorarios de abogados cuando una «agencia o componente federal designado» niegue la modificación de datos o deniegue el acceso a tales

[90] Anexo VII, p. 4.
[91] Anexo VII, p. 4.
[92] Proyecto de Decisión de adecuación, apartado 108.
[93] Ley de recurso judicial de 2015, H.R. 1428.

datos y el derecho a obtener reparaciones civiles en caso de divulgación de datos de forma deliberada o realizada voluntariamente.

Además, la jurisprudencia de los EE. UU. citada en las notas a pie de página de los considerandos pertinentes del proyecto de Decisión, en particular, City of Ontario/Quon[94], Maryland/King[95] y Samson/California[96], no es pertinente para apreciar si las personas no estadounidenses pueden reclamar ante los tribunales con el fin de impugnar la legalidad de una injerencia en su vida privada[97]. Todos los casos se refieren al derecho a la vida privada de ciudadanos estadounidenses, y todos ellos contienen resoluciones del Tribunal Supremo de los EE. UU. que, de hecho, limitan la aplicación de la Cuarta Enmienda.

En conjunto, el Grupo de trabajo del artículo 29 reconoce y acoge con satisfacción la adopción de la Ley de recurso judicial, pero sigue sin tener claro si realmente hay una tutela judicial efectiva a disposición de los interesados.

4.3 Observaciones finales

El Grupo de trabajo del artículo 29 acoge con satisfacción y reconoce el esfuerzo realizado por la administración de los EE. UU. para dar una visión más precisa del marco jurídico relativo a la injerencia en los datos personales comunicados en virtud del Escudo de la privacidad UE-EE. UU. a efectos de aplicación de la ley, incluidas las limitaciones y salvaguardias aplicables.

El Grupo de trabajo del artículo 29 constata que el sistema de instrumentos de investigación de las autoridades de aplicación de la ley, incluidas las limitaciones y garantías aplicables, es a la vez amplio y complejo y que la información incluida en el Escudo de la privacidad es breve. Así pues, el Grupo de trabajo del artículo 29 lamenta que, sobre la base de la limitada información (es decir, la información que se facilita en el anexo VII del Escudo de la privacidad y en las conclusiones del proyecto de Decisión), no le sea posible facilitar una evaluación global de la accesibilidad, la previsibilidad y la necesidad y proporcionalidad de las normas aplicables en este momento. Sin perjuicio de las demás conclusiones del Grupo de trabajo del artículo 29 sobre el Escudo de la privacidad incluidas en el presente dictamen, dicha evaluación podría integrarse en una revisión anual del Escudo de la privacidad.

Por lo que se refiere al acceso por parte de las fuerzas y cuerpos de seguridad, el Grupo de trabajo del artículo 29 señala que parece existir un mecanismo de supervisión independiente

[94] *City of Ontario, Cal./Quon*, 130 S. Ct. 2619, 2630 (2010).
[95] *Maryland/King*, 133 S. Ct. 1958, 1970 (2013).
[96] *Samson/California* (547 U.S. 848, 843 (2006).
[97] En *Ontario/Quon*, el Tribunal sostuvo que el Ayuntamiento de Ontario no vulneraba los derechos que la Cuarta Enmienda garantiza a sus trabajadores, pues el acceso del Ayuntamiento al contenido de los mensajes privados del trabajador en cuestión era razonable, ya que estaba motivado por un objetivo legítimo relacionado con el trabajo y no era excesivo en su alcance. En *Samson/California*, el Tribunal declaró que «la Cuarta Enmienda no prohíbe que un agente de policía lleve a cabo una investigación no basada en sospechas de un preso en libertad condicional». En *Maryland/King*, el Tribunal declaró que cuando los funcionarios llevan a cabo un arresto respaldado por una causa probable de retención de un sospechoso de un delito grave y lo conducen a la comisaría para mantenerlo detenido en custodia, realizar un frotis del ADN bucal del arrestado es, como la toma de huellas dactilares y la fotografía, un procedimiento policial legítimo que resulta razonable de conformidad con la Cuarta Enmienda.

bastante sólido. Además, el Grupo de trabajo del artículo 29 acoge con satisfacción la adopción de la Ley de recurso judicial, que concede derechos de recurso judicial a las personas no estadounidenses. No obstante, el Grupo de trabajo del artículo 29 señala que estos derechos son de naturaleza limitada. Además de la conclusión de que las personas no estadounidenses no estarían en condiciones de cuestionar las órdenes o requerimientos en el Tribunal invocando la Cuarta Enmienda, sigue preocupando la cuestión de si realmente existe una tutela judicial efectiva a disposición de los interesados en el ámbito de la aplicación de la ley.

5. CONCLUSIONES Y RECOMENDACIONES

En primer lugar, el Grupo de trabajo del artículo 29 acoge con satisfacción que en un plazo de cinco meses desde la invalidación del puerto seguro se presentase un nuevo proyecto de Decisión de adecuación con numerosas mejoras en comparación con el mecanismo anterior. Le complace especialmente el incremento de la transparencia que se ofrece a través de la introducción de dos listas del Escudo de la privacidad en la página web del DoC: una de los registros de entidades adheridas al Escudo de la privacidad y una de los registros de las entidades que han estado adheridas al Escudo pero ya no lo están. También se congratula de la mayor transparencia en relación con el acceso público a los datos transferidos en el marco del Escudo de la privacidad, ya sea con fines de seguridad nacional, o de aplicación de la ley. Por último, para el Grupo de trabajo del artículo 29 es una gran satisfacción saber que todas las transferencias de datos a los EE. UU. tendrán en adelante la misma protección: no existen disposiciones legales específicas que privilegien uno u otro instrumento.

5.1 Tres cuestiones preocupantes

No obstante, sigue habiendo tres cuestiones que preocupan al Grupo de trabajo del artículo 29, y que en su opinión habrá que abordar.

La primera preocupación es que el texto del proyecto de Decisión de adecuación no obliga a las entidades a suprimir los datos cuando ya no sean necesarios. Uno de los elementos fundamentales de la legislación de la UE sobre protección de datos es la garantía de que los datos se conserven durante un período no superior al necesario para la consecución de los fines para los que fueron recogidos. En segundo lugar, el Grupo de trabajo del artículo 29 entiende que, según el anexo VI, la administración estadounidense no excluye totalmente la recogida continuada de datos masivos e indiscriminados. El Grupo de trabajo del artículo 29 ha declarado reiteradamente que esta recogida de datos constituye una injerencia injustificada en los derechos fundamentales de los particulares. La tercera cuestión preocupante se refiere a la introducción del mecanismo del Defensor del Pueblo. Aunque el Grupo de trabajo del artículo 29 acoge con satisfacción esta iniciativa sin precedentes que crea un nuevo mecanismo de supervisión y de recurso para las particulares, siguen persistiendo dudas acerca de si el Defensor del Pueblo dispondrá de competencias suficientes para funcionar de manera eficaz. Como mínimo, las competencias y el cargo del Defensor del Pueblo deben explicarse, a fin de demostrar que su función es realmente independiente y puede ofrecer una tutela judicial efectiva en el caso del tratamiento de datos no conforme.

5.2 Aclaraciones recomendadas

Además de los puntos mencionados más arriba, el Grupo de trabajo del artículo 29 ha señalado a lo largo del presente dictamen varias cuestiones que precisan una mayor aclaración en la Decisión de adecuación. Y lo que es más importante, ello afecta a la necesidad de garantizar que los conceptos clave de la protección de datos utilizados en el Escudo de la privacidad se definan y apliquen de forma coherente. Actualmente, esto no es así. La integración de un glosario en las preguntas frecuentes del Escudo de la privacidad, preferiblemente con definiciones consensuadas entre la UE y los EE. UU., sería bien acogida. El Grupo de trabajo del artículo 29 señala también que las transferencias ulteriores de datos personales de la UE están insuficientemente reguladas, en particular en lo que respecta a su alcance, la limitación de su finalidad y las garantías aplicables a las transferencias a agentes. En cuanto al acceso a los datos del Escudo de la privacidad por parte de las fuerzas y cuerpos de seguridad, especialmente en lo que se refiere a la previsibilidad de la legislación, este constituye una preocupación, dadas la amplitud y la complejidad del sistema de aplicación de la Ley en los EE. UU., tanto a nivel federal como estatal, y la escasa información incluida en la Decisión de adecuación.

El Escudo de la privacidad es la primera Decisión de adecuación que se ha elaborado desde que los textos del Reglamento general de protección de datos se acordaron en principio. Sin embargo, muchas de las mejoras relativas a la protección de datos ofrecidas a los particulares no se recogen en el Escudo de la privacidad. Por tanto, el Grupo de trabajo del artículo 29 recomienda que, poco después de que entre en vigor el Reglamento general de protección de datos, se lleve a cabo una revisión de esta Decisión de adecuación, así como de las decisiones de adecuación emitidas por otros terceros países.

La recomendación final del Grupo de trabajo del artículo 29 que conviene destacar se refiere a la revisión conjunta. El Grupo de trabajo del artículo 29 acoge con satisfacción que la Decisión de adecuación del Escudo de la privacidad se revise anualmente, con una amplia participación de las APD y otras partes pertinentes. El Grupo de trabajo acogería con satisfacción un acuerdo sobre los elementos de las revisiones conjuntas, entre otras cosas sobre la elaboración y la presentación del informe de revisión, por todas las partes, con mucha antelación respecto de la primera revisión.