Recomendaciones

Recomendaciones 02/2020 sobre las garantías esenciales europeas para medidas de vigilancia

Adoptadas el 10 de noviembre de 2020

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Índice

El Comité Europeo de Protección de Datos

Visto el artículo 70, apartado 1, letra e), del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en lo sucesivo, «RGPD»),[1]

Visto el Acuerdo sobre el Espacio Económico Europeo y, en particular, su anexo XI y su Protocolo 37, modificado por la Decisión del Comité conjunto del EEE n.º 154/2018, de 6 de julio de 2018,[2]

Vistos los artículos 12 y 22 de su Reglamento interno,

Visto el documento de trabajo del Grupo de Trabajo del artículo 29 sobre la justificación de las injerencias en los derechos fundamentales a la intimidad y a la protección de datos a través de medidas de vigilancia al transferir datos personales (garantías esenciales europeas, en lo sucesivo «GEE»), WP237,

HA ADOPTADO LAS SIGUIENTES RECOMENDACIONES:

1. INTRODUCCIÓN

1. A raíz de la sentencia Schrems I, las autoridades de protección de datos de la UE reunidas en el Grupo de Trabajo 29 se basaron en la jurisprudencia para establecer las garantías esenciales europeas, que se han de respetar para asegurarse de que las injerencias en los derechos a la intimidad y a la protección de datos personales, a través de medidas de vigilancia, al transferir datos personales no exceden de lo necesario y proporcionado en una sociedad democrática.

2. El CEPD querría destacar que las garantías esenciales europeas se basan en la jurisprudencia del Tribunal de Justicia de la Unión Europea (en lo sucesivo, TJUE) en relación con los artículos 7, 8, 47 y 52 de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, la Carta) y, en su caso, en la jurisprudencia del Tribunal Europeo de Derechos Humanos (en lo sucesivo, TEDH) en relación con el artículo 8 del Convenio Europeo de Derechos Humanos (en lo sucesivo, CEDH) en materia de cuestiones de vigilancia en los Estados que son parte en el CEDH.[3]

[1] Este documento no trata las situaciones de transferencias o de comunicación ulterior que entran en el ámbito de la Directiva sobre protección de datos en el ámbito penal [Directiva (UE) 2016/680].

[2] Las referencias a los «Estados miembros» realizadas en el presente documento deben entenderse como referencias a los «Estados miembros del EEE».

[3] En estas Recomendaciones, el término «derechos fundamentales» dimana de la Carta de los Derechos Fundamentales de la Unión Europea. Sin embargo, se utiliza para referirse igualmente a los «derechos humanos» plasmados en el Convenio Europeo de Derechos Humanos.

3. La actualización de este documento pretende desarrollar en mayor medida las garantías esenciales europeas, redactadas originalmente en respuesta a la sentencia Schrems I[4], reflejando las aclaraciones proporcionadas por el TJUE (y por el TEDH) desde su primera publicación, en particular en su sentencia fundamental Schrems II.[5]

4. En su sentencia Schrems II, el TJUE declaró que el examen de la Decisión de la Comisión 2010/87/UE relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, a la luz de los artículos 7, 8 y 47 de la Carta, no ha revelado nada que afecte a la validez de dicha Decisión, pero en cambio invalidó la Decisión sobre el Escudo de la privacidad. El TJUE sostuvo que la Decisión sobre el Escudo de la privacidad era incompatible con el artículo 45, apartado 1, del RGPD, a la luz de los artículos 7, 8 y 47 de la Carta. La sentencia puede así servir de ejemplo de los casos en los que las medidas de vigilancia en un tercer país (en este caso, Estados Unidos con el artículo 702 de la FISA y la Executive Order 12333) no están lo suficientemente limitadas ni están sujetas a un recurso efectivo a disposición de los interesados para que ejerzan sus derechos, como impone el Derecho de la Unión a fin de considerar el nivel de protección en un tercer país «esencialmente equivalente» al garantizado en la Unión Europea en el sentido del artículo 45, apartado 1, del RGPD.

5. Las razones para la invalidación del Escudo de la privacidad tienen también consecuencias en otras herramientas de transferencia[6]. Aunque el Tribunal interpretó el artículo 46, apartado 1, del RGPD en el contexto de la validez de las cláusulas contractuales tipo (en lo sucesivo, CCT), su interpretación se aplica a cualquier transferencia a terceros países basada en cualquiera de las herramientas mencionadas en el artículo 46 del RGPD.[7]

6. En última instancia, compete al TJUE juzgar si se pueden justificar las injerencias en un derecho fundamental. Sin embargo, en ausencia de una sentencia al respecto y en aplicación de reiterada jurisprudencia, las autoridades de protección de datos deben apreciar los casos de forma individual, ya sea de oficio o a raíz de una reclamación, y derivarlos a un órgano jurisdiccional nacional si sospechan que la transferencia no cumple con el artículo 45 en concurrencia de una decisión de adecuación, o bien suspender o prohibir la transferencia si concluyen que no se puede cumplir el artículo 46 del RGPD y no se puede asegurar por otros medios la protección de los datos transferidos impuesta por el Derecho de la Unión.

7. El objetivo de las garantías esenciales europeas actualizadas es proporcionar elementos para examinar si las medidas de vigilancia que permiten el acceso a datos personales por parte de las autoridades públicas de un tercer país, ya sean agencias de seguridad nacional o fuerzas o cuerpos de seguridad, se pueden considerar o no una injerencia justificable.

[4] Sentencia del TJUE de 6 de octubre de 2015, Maximillian Schrems/Data Protection Commissioner, asunto C-362/14, EU:C:2015:650 (en lo sucesivo, Schrems I).

[5] Sentencia del TJUE de 16 de julio de 2020, Data Protection Commissioner/Facebook Ireland Limited y Maximillian Schrems, asunto C-311/18, ECLI:EU:C:2020:559 (en lo sucesivo, Schrems II).

[6] Véase el apartado 105 de Schrems II.

[7] Véase el apartado 92 de Schrems II.

8. De hecho, las garantías esenciales europeas forman parte de la apreciación que se ha de llevar a cabo a fin de determinar si un tercer país ofrece un nivel de protección esencialmente equivalente al garantizado en la Unión, pero no pretenden definir por sí mismas todos los elementos necesarios para considerar que un tercer país proporciona dicho nivel de protección de conformidad con el artículo 45 del RGPD. De igual manera, tampoco están encaminadas a determinar por sí solas todos los elementos que cabría considerar al evaluar si el ordenamiento jurídico de un tercer país impide al exportador y al importador de los datos proporcionar unas garantías adecuadas con arreglo al artículo 46 del RGPD.

9. Por lo tanto, los elementos dispuestos en el presente documento se han de considerar garantías esenciales que el tercer país deberá presentar al apreciar la injerencia, provocada por las medidas de vigilancia de un tercer país, con los derechos a la intimidad y a la protección de datos, y no una lista de elementos para demostrar que el ordenamiento jurídico de un tercer país en su conjunto ofrece un nivel de protección esencialmente equivalente.

10. El artículo 6, apartado 3, del Tratado de la Unión Europea establece que los derechos fundamentales consagrados en el CEDH constituyen principios generales del Derecho de la Unión. Sin embargo, como el TJUE recuerda en su jurisprudencia, dicho Convenio no constituye, en la medida en que la Unión Europea no lo haya suscrito, un instrumento jurídico incorporado formalmente al Derecho de la Unión.[8] De tal manera, el nivel de protección de los derechos fundamentales exigido por el artículo 46, apartado 1, del RGPD debe determinarse en función de las disposiciones de dicho Reglamento, leído a la luz de los derechos fundamentales consagrados en la Carta. Dicho esto, de acuerdo con el artículo 52, apartado 3, de la Carta, los derechos en ella plasmados que se corresponden con derechos garantizados por el CEDH deben tener el mismo significado y alcance que los dispuestos por dicho Convenio y, en consecuencia, como ha recordado el TJUE, la jurisprudencia del TEDH sobre derechos también previstos en la Carta de los Derechos Fundamentales de la Unión Europea se ha de tener en cuenta como umbral mínimo de protección para interpretar los derechos correspondientes de la Carta.[9] Sin embargo, con arreglo a la última frase del artículo 52, apartado 3, de la Carta, «[e]sta disposición no impide que el Derecho de la Unión conceda una protección más extensa».

11. En consecuencia, la sustancia de las garantías esenciales seguirá basándose en parte en la jurisprudencia del TEDH en la medida en que la Carta, según su interpretación por el TJUE, no disponga un mayor nivel de protección que prescriba otros requisitos que la jurisprudencia del TEDH.

12. En el presente documento se explica el trasfondo de las garantías esenciales europeas y se procede a detallarlas en mayor medida.

[8] Véase el apartado 98 de Schrems II.

[9] Véase el apartado 124 de los asuntos acumulados C-511/18, C-512/18 y C-520/18, La Quadrature du Net y otros (en lo sucesivo, La Quadrature du Net y otros).

2. INJERENCIAS EN LOS DERECHOS FUNDAMENTALES

13. Los derechos fundamentales al respeto de la vida privada y familiar, incluidas las comunicaciones, y a la protección de los datos personales se encuentran plasmados en los artículos 7 y 8 de la Carta y se aplican a todas las personas. Por añadidura, el artículo 8 establece condiciones para que el tratamiento de datos personales sea legítimo, reconoce el derecho de acceso y de rectificación e impone además que estas normas estén sujetas al control de una autoridad independiente.

14. «(L)a operación consistente en hacer transferir datos personales desde un Estado miembro a un tercer país constituye por sí misma un tratamiento de datos personales».[10] Así, los artículos 7 y 8 de la Carta se aplican a esta operación específica y su protección se extiende a los datos transferidos, razón por la cual los interesados cuyos datos personales se transfieran a un tercer país deben recibir un nivel de protección esencialmente equivalente al garantizado en la Unión Europea.[11]

15. Según el TJUE, cuando el derecho fundamental al respeto a la vida privada consagrado en el artículo 7 de la Carta se ve afectado en razón del tratamiento de los datos personales de una persona, tal extremo incide asimismo en el derecho a la protección de datos, puesto que dicho tratamiento entra dentro del ámbito de aplicación del artículo 8 de la Carta y, en consecuencia, debe cumplir necesariamente el requisito de protección de datos dispuesto en el mismo.[12]

16. Por consiguiente, en lo concerniente a la posible injerencia en los derechos fundamentales en virtud del Derecho de la Unión, la obligación impuesta a los prestadores de servicios de comunicaciones electrónicas [...] de conservar datos sobre el tráfico a efectos de ponerlos en su caso a disposición de las autoridades nacionales competentes plantea problemas de compatibilidad con los artículos 7 y 8 de la Carta.[13.] Lo mismo resulta de aplicación a otros tipos de tratamiento de datos, como la transmisión de datos a personas diferentes de los usuarios o el acceso a dichos datos con vistas a su uso[14], que, de tal suerte, comportan una injerencia en los derechos fundamentales en cuestión. Por añadidura, de conformidad con la jurisprudencia consolidada,[15] el acceso a los datos por parte de una autoridad pública constituye otra injerencia más.

17. A fin de detectar una injerencia, carece de relevancia que «la información relativa a la vida privada de que se trate tenga o no carácter sensible o [que] los interesados hayan sufrido o no inconvenientes en razón de tal injerencia».[16] El TJUE recalcó asimismo que carecía de relevancia si los datos conservados se habían utilizado ulteriormente o no.[17]

18. No obstante, los artículos 7 y 8 de la Carta no son derechos absolutos, sino que se han de considerar en relación con su función en la sociedad.[18]

---

[10] TJUE, Schrems II, apartado 83.
[11] TJUE, Schrems II, apartado 96.
[12] TJUE, Schrems II, apartados 170 y 171.
[13] TJUE, asunto C-623/17, Privacy International (en lo sucesivo, Privacy International), apartado 60.
[14] TJUE, Privacy International, apartado 61.
[15] TEDH, Leander, apartado 48; TEDH, Rotaru, apartado 46; TJUE, Digital Rights Ireland, apartado 35.
[16] TJUE, Schrems II, apartado 171, y la jurisprudencia citada.
[17] TJUE, Schrems II, apartado 171, y la jurisprudencia citada.
[18] TJUE, Privacy International, apartado 63.

19. La Carta incluye una prueba de la necesidad y la proporcionalidad para acotar las limitaciones a los derechos que protege. En el artículo 52, apartado 1, de la Carta se especifica el alcance de las posibles limitaciones a los artículos 7 y 8 al indicar que «[c]ualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por ley y respetar el contenido esencial de dichos derechos y libertades. Solo se podrán introducir limitaciones, respetando el principio de proporcionalidad, cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás».

20. El TJUE reiteró que la legislación de la Unión que conlleve una injerencia en los derechos fundamentales garantizados por los artículos 7 y 8 de la Carta «debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas, de modo que las personas cuyos datos se hayan conservado dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso», en particular cuando los datos personales se someten a un tratamiento automatizado y «cuando existe un riesgo elevado de acceso ilícito a dichos datos».[19]

21. De acuerdo con el TJUE, la protección del derecho a la intimidad requiere que las excepciones y las limitaciones del derecho a la protección de datos «se establezcan sin sobrepasar los límites de lo estrictamente necesario». Otrosí, un objetivo de interés general se debe conciliar con los derechos fundamentales afectados por la medida y «debe efectuarse una ponderación equilibrada» del mismo con los derechos en cuestión.[20]

22. Por consiguiente, el acceso, la conservación y el uso posterior de datos personales por las autoridades públicas en el ámbito de medidas de vigilancia no deben exceder de los límites de lo estrictamente necesario, demarcados a la luz de la Carta, puesto que, de lo contrario, «no puede[n] considerarse justificad[os] en una sociedad democrática».[21]

23. Las cuatro garantías esenciales europeas desarrolladas en el siguiente capítulo pretenden concretar aún más la forma de apreciar el nivel de injerencia en los derechos fundamentales a la intimidad y a la protección de datos en el contexto de medidas de vigilancia aplicadas por las autoridades públicas en un tercer país, al transferir datos personales, y qué requisitos jurídicos deben en consecuencia aplicarse a fin de ponderar si dichas injerencias serían aceptables en virtud de la Carta.

3. LAS GARANTÍAS ESENCIALES EUROPEAS

24. A raíz del análisis de la jurisprudencia, el CEPD considera que los requisitos jurídicos aplicables para que sean justificables las limitaciones a los derechos a la protección de datos y a la intimidad reconocidos por la Carta se pueden resumir en cuatro garantías esenciales europeas:

A. El tratamiento se debe basar en normas claras, precisas y accesibles
B. Se tiene que demostrar la necesidad y la proporcionalidad con respecto a los objetivos legítimos
C. Debe existir un mecanismo de supervisión independiente

[19] TJUE, Privacy International, apartado 68, y la jurisprudencia citada.
[20] TJUE, Privacy International, apartado 68, y la jurisprudencia citada.
[21] TJUE, Privacy International, apartado 81.

D. El interesado debe tener a su disposición recursos efectivos

25. Las garantías se basan en los derechos fundamentales a la intimidad y a la protección de datos que amparan a todas las personas, con independencia de su nacionalidad.

Garantía A: el tratamiento se debe basar en normas claras, precisas y accesibles

26. De conformidad con el artículo 8, apartado 2, de la Carta, los datos personales deben, entre otras cosas, tratarse «para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley»,[22] como el TJUE recuerda en su sentencia Schrems II. Además, con arreglo al artículo 52, apartado 1, de la Carta, cualquier limitación del ejercicio de los derechos y libertades reconocidos por la Carta en la Unión deberá ser establecida por la ley. Por ende, una injerencia justificable tiene que ajustarse a Derecho.

27. Esta base jurídica debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión y establezcan unas exigencias mínimas.[23] Por añadidura, el Tribunal recordó que la «normativa debe ser legalmente imperativa en Derecho interno».[24] Al respecto, el TJUE aclaró que la apreciación del Derecho aplicable del tercer país debe centrarse en si los interesados lo pueden invocar ante un órgano jurisdiccional[25]. Por tanto, el Tribunal indica que los derechos concedidos a los interesados deben ser exigibles; si a los interesados no se les conceden derechos protegidos jurídicamente contra los poderes públicos, no se podrá considerar que el nivel de protección otorgado es esencialmente equivalente al dimanante de la Carta, en contra del requisito establecido en el artículo 45, apartado 2, letra a), del RGPD.[26]

28. Además, el Tribunal destacó que el Derecho aplicable debe indicar en qué circunstancias y con arreglo a qué condiciones se podría adoptar una medida que dispusiera el tratamiento de dichos datos[27] (véase más adelante, en la Garantía B, la relación entre estos requisitos y los principios de necesidad y proporcionalidad).

29. Por añadidura, el TJUE ha indicado también que «el requisito de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que permita la injerencia en dichos derechos debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate».[28]

30. Finalmente, el Tribunal Europeo de Derechos Humanos «no considera que exista ninguna razón para aplicar unos principios diferentes respecto a la accesibilidad y claridad de las normas que rigen la intervención de las comunicaciones individuales, de un lado, y a programas de vigilancia más generales,

[22] Véase el apartado 173 de Schrems II.

[23] Véanse los apartados 175 y 180 de Schrems II y el Dictamen 1/15 (Acuerdo PNR entre la UE y Canadá) de 26 de julio de 2017, apartado 139, y la jurisprudencia citada.

[24] Véase el apartado 68 de Privacy International. Cabe reseñar que en la versión francesa de la sentencia el Tribunal de Justicia utiliza la palabra «*réglementation*», que tiene un sentido más amplio que los actos del Parlamento.

[25] Véase el apartado 181 de Schrems II, donde el TJUE alude a la Directiva de Política Presidencial 28 de EE. UU.

[26] Véase el apartado 181 de Schrems II.

[27] Véase el apartado 68 de Privacy International, en relación con el Derecho del Estado miembro.

[28] Véase Schrems II, apartado 175, y la jurisprudencia citada, así como Privacy International, apartado 65.

de otro»[29]. El TEDH también ha aclarado que la base jurídica debe incluir al menos una definición de las categorías de personas que podrían ser sometidas a vigilancia, un límite de duración de la medida, el procedimiento que se ha de seguir para examinar, utilizar y conservar los datos obtenidos y las cautelas de obligada adopción al comunicar los datos a terceros.[30]

31. Por último, el efecto de la injerencia debe ser previsible para el interesado, a fin de brindarle una protección adecuada y efectiva contra las injerencias arbitrarias y los riesgos de abuso. Por ende, el tratamiento se debe fundamentar en una base jurídica precisa y clara, pero también accesible (es decir, pública).[31] En relación con esta cuestión, el TEDH recordó en el asunto Zakharov que «la referencia a la "previsibilidad" en el contexto de la interceptación de comunicaciones no puede ser la misma que en muchos otros ámbitos». Especificó que en el contexto de medidas de vigilancia secretas, como la interceptación de comunicaciones, «la previsibilidad no puede significar que una persona deba poder prever cuándo es probable que las autoridades intercepten sus comunicaciones para así poder adaptar su conducta en consecuencia». Sin embargo, considerando que en este tipo de situaciones son evidentes los riesgos de arbitrariedad, «es esencial contar con normas claras y detalladas sobre la interceptación de conversaciones telefónicas, especialmente porque la tecnología disponible para dichas operaciones es cada vez más sofisticada. La legislación nacional debe ser suficientemente clara para ofrecer a los ciudadanos una indicación adecuada de las circunstancias y condiciones en las que las autoridades públicas están facultadas para recurrir a tales medidas».[32]

Garantía B: se tiene que demostrar la necesidad y la proporcionalidad con respecto a los objetivos legítimos

32. De conformidad con la primera frase del artículo 52, apartado 1, de la Carta, cualquier limitación del ejercicio de los derechos y libertades reconocidos por la Carta debe respetar el contenido esencial de dichos derechos y libertades. En virtud de la segunda frase del artículo 52, apartado 1, de la Carta, solo se podrán introducir limitaciones a dichos derechos y libertades respetando el principio de proporcionalidad, cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás.[33]

33. Con respecto al **principio de proporcionalidad**, el Tribunal sostuvo, en relación con el Derecho de los Estados miembros, que la cuestión de si podía estar justificada una limitación de los derechos a la intimidad y a la protección de los datos se debe apreciar, por una parte, ponderando la **gravedad de la injerencia** acarreada por dicha limitación[34] y, por otra, verificando que la **importancia del objetivo de interés público** perseguido por la limitación sea proporcionada a dicha gravedad.[35]

[29] TEDH, Liberty, apartado 63.

[30] TEDH, Weber y Saravia, apartado 95.

[31] TEDH, Malone, apartados 65 y 66.

[32] TEDH, Zakharov, apartado 229.

[33] Schrems II, apartado 174.

[34] En este contexto, el Tribunal reseñó por ejemplo que «parece especialmente grave la injerencia que representa la recogida en tiempo real de datos que permiten la localización de equipos terminales, puesto que dichos datos les proporcionan a las autoridades nacionales competentes un medio de rastrear de una manera precisa y permanente los movimientos de los usuarios de telefonía móvil [...]». (La Quadrature du Net y otros, apartado 187, y la jurisprudencia citada).

[35] La Quadrature du Net y otros, apartado 131.

34. En La Quadrature du Net y otros, se puede observar que el TJUE dictaminó, en relación con el Derecho de un Estado miembro —no de un tercer país—, que el objetivo de proteger la seguridad nacional puede en razón de su importancia justificar medidas que comportan injerencias más graves en derechos fundamentales que las que podrían verse justificadas por otras metas, como la de la lucha contra la delincuencia. Concluyó no obstante que tal es el caso siempre que haya unos motivos lo suficientemente sólidos como para considerar que el Estado interesado se enfrenta a una amenaza grave para la seguridad nacional, que se demuestre auténtica y existente o previsible, y de manera supeditada a cumplir el resto de requisitos dispuestos en el artículo 52, apartado 1, de la Carta.[36]

35. A este respecto, de conformidad con reiterada jurisprudencia, las excepciones y las limitaciones de la protección de datos personales solo se deberán aplicar en la medida en que sean estrictamente necesarias.[37] Para satisfacer este requisito, además de establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión, la legislación debe imponer unas exigencias mínimas, de modo que las personas cuyos datos se hayan transferido dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso. «En particular, dicha normativa deberá indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de tales datos, garantizando así que la injerencia se limite a lo estrictamente necesario. La necesidad de disponer de tales garantías reviste especial importancia cuando los datos personales se someten a un tratamiento automatizado».[38]

36. En Schrems II, el TJUE destacó que la legislación de un tercer país que no indique ninguna limitación al poder que confiere para instaurar programas de vigilancia con fines de inteligencia extranjera no puede garantizar un nivel de protección esencialmente equivalente al garantizado por la Carta. De hecho, de conformidad con la jurisprudencia, para cumplir los requisitos del principio de proporcionalidad, una base jurídica que permite la injerencia en derechos fundamentales debe definir el alcance de la limitación del ejercicio del derecho en cuestión.[39]

37. Con respecto al **principio de necesidad**, el TJUE ha dejado claro que las legislaciones «que autorizan de forma generalizada la conservación de la totalidad de los datos personales de todas las personas cuyos datos se hayan transferido desde la Unión Europea [...] sin establecer ninguna diferenciación, limitación o excepción en función del objetivo perseguido y sin prever ningún criterio objetivo que permita circunscribir el acceso de las autoridades públicas a los datos y su utilización posterior a fines específicos, estrictamente limitados y propios para justificar la injerencia que constituyen tanto el

[36] Apartados 136 y 137. Véase también Privacy International; como especificó el Tribunal, dichas amenazas se pueden distinguir, por su naturaleza y especial gravedad, del riesgo general de que surjan tensiones o desórdenes, incluso graves, que afecten a la seguridad nacional. Apartado 75. Por ejemplo, en La Quadrature du Net y otros, el Tribunal observó que un análisis automatizado de datos de tráfico y localización que abarque de manera general e indiscriminada los datos de usuarios de sistemas de comunicaciones electrónicas constituye una injerencia especialmente grave, de manera que dicha medida solo puede cumplir el requisito de proporcionalidad en situaciones en las que el Estado miembro interesado se enfrente a una amenaza grave para la seguridad nacional que se demuestre auténtica y existente o previsible y, entre otras condiciones, siempre que la duración de la conservación se limite a lo estrictamente necesario (apartados 174 a 177).

[37] Schrems II, apartado 176, y la jurisprudencia citada.

[38] Schrems II, apartado 175.

[39] Schrems II, apartado 180.

acceso a esos datos como su utilización» no cumplen dicho principio.[40] En particular, ha de considerarse que las leyes que permiten que las autoridades públicas tengan acceso, con carácter general, al contenido de las comunicaciones electrónicas lesionan el contenido esencial del derecho fundamental al respeto de la vida privada garantizado por el artículo 7 de la Carta.[41]

38. De igual modo, aunque en esta ocasión al apreciar el Derecho de un Estado miembro y no el de un tercer país, el TJUE sostuvo en La Quadrature du Net y otros que «la legislación que imponga la conservación de datos personales debe cumplir siempre criterios objetivos que establezcan una relación entre los datos conservados y el objetivo perseguido».[42] En el mismo contexto, en Privacy International, mantuvo asimismo que el legislador «debe basarse en criterios objetivos para definir las circunstancias y los requisitos conforme a los cuales debe concederse a las autoridades nacionales competentes el acceso a los datos de que se trate».[43]

Garantía C: mecanismo de supervisión independiente

39. El CEPD recuerda que una injerencia tiene lugar tanto en el momento de la recogida de los datos como en el que la autoridad pública accede a ellos para su ulterior tratamiento. El TEDH ha especificado en numerosas ocasiones que cualquier injerencia en el derecho a la intimidad y a la protección de datos debe ser objeto de un sistema de supervisión eficaz, independiente e imparcial por parte de un juez u otro organismo independiente[44] (p. ej., una autoridad administrativa o una instancia parlamentaria). El TJUE también tuvo en cuenta la supervisión independiente de la aplicación de las medidas de vigilancia en la sentencia Schrems II.[45]

[40] Schrems I, apartado 93, con referencias adicionales. Véase, no obstante esta vez en relación con el Derecho de un Estado miembro y no el de un tercer país, Privacy International, apartado 71, y la jurisprudencia citada. En este caso, el Tribunal declaró que la legislación de un Estado miembro que obliga a los prestadores de servicios de comunicaciones electrónicas a divulgar datos de tráfico y localización a las agencias de seguridad e inteligencia por medio de una transmisión general e indiscriminada excede de los límites de lo estrictamente necesario y no se puede considerar justificada en una sociedad democrática, conforme requiere la Directiva sobre la privacidad y las comunicaciones electrónicas, leída a la luz de la Carta (apartado 81).

[41] Schrems I, apartado 94.

[42] La Quadrature du Net y otros, apartado 133. En este contexto, el Tribunal de Justicia confirmó que las medidas legislativas que disponen con carácter preventivo la conservación general e indiscriminada de datos de tráfico y localización quedan excluidas por la Directiva sobre la privacidad y las comunicaciones electrónicas, leída a la luz de la Carta. Por el contrario, el Tribunal resolvió que, en situaciones de una amenaza grave a la seguridad nacional, que se demuestre auténtica y existente o previsible, el legislador, para proteger dicha seguridad nacional, podrá permitir el recurso a una instrucción que obligue a los prestadores de servicios de comunicaciones electrónicas a conservar, de manera general e indiscriminada, datos de tráfico y localización. Sin embargo, dicha medida debe cumplir unas condiciones específicas. En particular, la instrucción solo se podrá dar para un período temporal limitado a lo estrictamente necesario, que se podrá prorrogar en el supuesto de persistencia de la amenaza (apartado 168).

[43] Privacy International, apartado 78, y la jurisprudencia citada. En Privacy International, en cuanto al acceso de una autoridad a datos personales proporcionados con arreglo al Derecho de un Estado miembro, el Tribunal declaró que «un acceso general a todos los datos conservados, con independencia de la existencia de una relación, por lo menos indirecta, con el fin perseguido, no puede considerarse limitado a lo estrictamente necesario» (apartados 77 y 78).

[44] TEDH, Klass, apartados 17 y 51.

[45] Schrems II, apartados 179 y 183.

40. El TEDH especifica que aunque la autorización (judicial) previa de las medidas de vigilancia es una importante garantía contra la arbitrariedad, se ha prestar atención asimismo al funcionamiento efectivo del sistema de interceptación, incluido el sistema de contrapesos para el ejercicio del poder y la existencia o la ausencia de abusos efectivos.[46] En el asunto Schrems II, el TJUE tuvo en consideración asimismo el alcance de la función de control del mecanismo de supervisión, que no abarcaba las medidas de vigilancia individuales.[47]

41. Con respecto al Derecho de los Estados miembros, el TJUE determinó una serie de medidas que solo cumplen con el Derecho de la Unión si se someten a un control efectivo por parte de un órgano jurisdiccional o una autoridad administrativa independiente cuyas decisiones sean vinculantes. El objetivo de dicho control es verificar la existencia de una situación que justifique la medida y el cumplimiento de las condiciones y las garantías que se han de disponer.[48] Para la recogida en tiempo real de datos de tráfico y localización, el control debe permitir verificar *a priori*, entre otras cosas, si está autorizada solo en la medida de lo estrictamente necesario. En supuestos de urgencia debidamente justificada, las medidas pueden aplicarse sin dicho control previo; no obstante, el Tribunal sigue requiriendo que el control posterior se realice con rapidez.[49]

42. En cuanto a la independencia de los mecanismos de supervisión en relación con la vigilancia, se podrían tener en cuenta las conclusiones del TJUE acerca de la independencia de un organismo en el contexto de las vías de recurso (véase más adelante la Garantía D). Por otra parte, la jurisprudencia del TEDH podría ofrecer elementos adicionales. Este Tribunal ha expresado su preferencia por que un juez sea el responsable de la supervisión y su mantenimiento. Empero, no se descarta que pueda hacerse responsable otro órgano, «siempre que sea lo suficientemente independiente del Ejecutivo»[50] y «de las autoridades encargadas de la vigilancia y tenga poderes y competencias suficientes para ejercer un control efectivo y continuo».[51] El TEDH añadió que al apreciar la independencia se habían de tener en cuenta «la manera de designación y el estatuto jurídico de los miembros del órgano de control»[52]. Entre ellos se incluyen las «personas cualificadas para ejercer una función jurisdiccional, designadas por el Parlamento o por el Primer Ministro. En cambio, se estimó que un Ministro del Interior —quien no solo era una persona nombrada políticamente y miembro del Ejecutivo, sino que estuvo directamente implicado en la puesta en marcha de medios especiales de vigilancia— era insuficientemente independiente».[53] El TEDH, además, «observa que es esencial que el órgano de control tenga acceso a todos los documentos pertinentes, incluidos los reservados».[54] Finalmente, el TEDH tiene en cuenta «si las actividades del órgano de control están abiertas al escrutinio público».[55]

[46] TEDH, Big Brother Watch en apelación, apartados 319 y 320.

[47] Schrems II, apartado 179.

[48] TJUE, La Quadrature du Net y otros, apartados 168 y 189.

[49] TJUE, La Quadrature du Net y otros, apartado 189.

[50] TEDH, Zakharov, apartado 258, Iordachi y otros/Moldavia, apartados 40 y 51, y Dumitru Popescu/Rumanía, apartados 70 a 73.

[51] TEDH, Klass, apartado 56, y Big Brother Watch en apelación, apartado 318.

[52] TEDH, Zakharov, apartado 278.

[53] TEDH, Zakharov, apartado 278.

[54] TEDH, Zakharov, apartado 281.

[55] TEDH, Zakharov, apartado 283.

Garantía D: el interesado debe tener a su disposición recursos efectivos

43. La última garantía esencial europea está relacionada con las vías de recurso del interesado. Este debe contar con un recurso efectivo para ejercer sus derechos cuando considere que no se han respetado. El TJUE explicó en Schrems I que «una normativa que no prevé posibilidad alguna de que el justiciable ejerza acciones en Derecho para acceder a los datos personales que le conciernen o para obtener su rectificación o supresión no respeta el contenido esencial del derecho fundamental a la tutela judicial efectiva que reconoce el artículo 47 de la Carta. En efecto, el artículo 47, párrafo primero, de ésta establece que toda persona cuyos derechos y libertades garantizados por el Derecho de la Unión hayan sido violados tiene derecho a la tutela judicial efectiva, respetando las condiciones establecidas en dicho artículo».[56]

44. Al apreciar el Derecho de un Estado miembro que permite la recogida de datos de tráfico y localización, el Tribunal consideró que la notificación es necesaria «para permitirles a las personas afectadas ejercer sus derechos contemplados en los artículos 7 y 8 de la Carta a solicitar acceso a sus datos personales objeto de dichas medidas y, si procede, a su rectificación o supresión, así como a valerse de un recurso judicial efectivo, de conformidad con el apartado primero del artículo 47 de la Carta».[57] No obstante, también reconoció que la notificación a personas cuyos datos se hayan recogido o analizado se ha de producir solo en la medida y en el momento en que dicha notificación ya no ponga en peligro las tareas de las que son responsables las autoridades de que se trate.[58]

45. Para el TEDH, la cuestión de un recurso efectivo también está inextricablemente vinculada a la notificación de la medida de vigilancia al interesado una vez se haya levantado esta. En particular, el Tribunal concluyó que «en principio, el interesado tiene escaso margen para el recurso judicial, a menos que se le informe de las medidas tomadas sin su conocimiento y de tal suerte pueda oponerse a su legalidad de manera retrospectiva o, como alternativa, a menos que cualquier persona que sospeche que sus comunicaciones están siendo interceptadas pueda recurrir a los órganos jurisdiccionales, para que la competencia de los tribunales no dependa de la notificación al interesado de la interceptación de sus comunicaciones»[59]. Así, el TEDH reconoció que, aunque en algunos casos podría no haber notificación, se debe proporcionar no obstante un recurso efectivo. En este caso, este Tribunal ha dejado claro, por ejemplo en el asunto Kennedy, que un órgano jurisdiccional ofrece suficientes vías de recurso si cumple una serie de criterios, o sea, es un órgano independiente e imparcial, que ha adoptado su propio reglamento de procedimiento y está compuesto por miembros que deben ejercer o haber ejercido una función jurisdiccional o ser abogados experimentados y no hay una carga probatoria que superar a fin de presentar una solicitud ante él.[60] Al acometer su examen de las reclamaciones de los

[56] TJUE, Schrems I, apartado 95.
[57] Véase el apartado 190 de La Quadrature du Net y otros y TJUE, Dictamen 1/15, apartado 220.
[58] Véase el apartado 191 de La Quadrature du Net y otros.
[59] TEDH, Zakharov, apartado 234.
[60] TEDH, Kennedy, apartado 190.

interesados, el órgano jurisdiccional debe tener acceso a toda la información pertinente,[61] incluida la reservada. Finalmente, deber tener los poderes necesarios para reparar los incumplimientos.[62]

46. El artículo 47 de la Carta se refiere a un tribunal, aunque en otras versiones lingüísticas distintas del inglés se ha dado preferencia al término «*court*»,[63] mientras que el CEDH solo obliga a los Estados miembros a garantizar que «todas las personas cuyos derechos y libertades hayan sido violados dispongan de un recurso efectivo ante una autoridad nacional»,[64] que no tiene que ser necesariamente una autoridad judicial.[65]

47. El TJUE, en el contexto de la sentencia Schrems II, al apreciar la adecuación del nivel de protección de un tercer país, ha reiterado que «los justiciables han de tener la posibilidad de ejercer acciones en Derecho ante un tribunal independiente e imparcial para acceder a los datos personales que les conciernen o para obtener su rectificación o supresión».[66] En el mismo contexto, el TJUE considera que la tutela judicial efectiva contra tales injerencias no solo la puede asegurar un órgano jurisdiccional, sino también un órgano[67] que ofrezca garantías esencialmente equivalentes a las establecidas por el artículo 47 de la Carta. En su sentencia Schrems II, el TJUE subrayó tanto que se ha de garantizar la independencia del tribunal o el órgano, especialmente del Ejecutivo, con todas las garantías necesarias, incluido en relación con sus condiciones de destitución o revocación del nombramiento,[68] como que los poderes que se deben conceder a un tribunal tienen que cumplir los requisitos del artículo 47 de la Carta. A este respecto, al órgano[69] se le concederá el poder de adoptar decisiones vinculantes sobre los servicios de inteligencia, de conformidad con las garantías jurídicas en las que pueden basarse los interesados.[70]

4. OBSERVACIONES FINALES

48. Las cuatro garantías esenciales europeas se han de considerar como los elementos clave cuya existencia se ha de dilucidar al apreciar el nivel de injerencia en los derechos fundamentales a la intimidad y la protección de datos. Comoquiera que están estrechamente entrelazadas, no se deben valorar independientemente, sino de una manera global, analizando la legislación pertinente en relación con las medidas de vigilancia, el nivel mínimo de garantías para la protección de los derechos de los interesados y las vías de recurso dispuestas en el Derecho nacional del tercer país.

---

[61] El CEPD observa que el Comisario para los Derechos Humanos del Consejo de Europa considera que la denominada regla de «terceros», en virtud de la cual las agencias de inteligencia de un país que proporcionen datos a agencias de inteligencia de otro país pueden imponerles la obligación de no divulgar los datos transferidos a ningún tercero no debe aplicarse a los órganos de control a fin de no socavar la posibilidad de un recurso efectivo (Documento de debate sobre el control democrático y eficaz de los servicios de seguridad nacionales).

[62] TEDH, Kennedy, apartado 167.

[63] Por ejemplo, la palabra *«tribunal»* en inglés se traduce como «*Gericht*» en alemán y «*gerecht*» en neerlandés.

[64] Artículo 13 del CEDH.

[65] TEDH, Klass, apartado 67.

[66] Véase el apartado 194 de Schrems II.

[67] Véase el apartado 197 de Schrems II, en el que el Tribunal de Justicia utiliza expresamente este término.

[68] Véase el apartado 195 de Schrems II.

[69] Véase el apartado 197 de Schrems II, en el que el Tribunal de Justicia utiliza expresamente este término.

[70] Véase el apartado 196 de Schrems II.

49. Estas garantías requieren un cierto grado de interpretación, especialmente porque la legislación del tercer país no tiene que ser idéntica al marco jurídico de la Unión.

50. Como el TEDH declaró en el asunto Kennedy, una «apreciación dependerá de las circunstancias que concurran en el caso, por ejemplo, la naturaleza, amplitud y duración de las eventuales medidas, las razones que justifiquen acordar tales medidas, las autoridades competentes para autorizarlas, ejecutarlas y controlarlas, así como el tipo de recursos que el Derecho interno permita interponer».[71]

51. En consecuencia, el cotejo de las medidas de vigilancia del tercer país con las GEE puede conducir a dos conclusiones:

- La legislación del tercer país en cuestión no garantiza los requisitos de las GEE: en este supuesto, el Derecho del tercer país no ofrecería un nivel de protección esencialmente equivalente al garantizado en la Unión.

- La legislación del tercer país en cuestión sí satisface las GEE.

52. Al ponderar la adecuación del nivel de protección en virtud del artículo 45 del RGPD, la Comisión habrá de apreciar si las GEE se satisfacen como parte de los elementos que se han de considerar para asegurarse de que la legislación del tercer país, en su conjunto, ofrece un nivel de protección esencialmente equivalente al garantizado en la Unión.

53. Si los exportadores y los importadores de datos se basan en las garantías oportunas en virtud del artículo 46 del RGPD, teniendo en cuenta los requisitos de la legislación del tercer país aplicables específicamente a los datos transferidos, tendrán que asegurar que se logra efectivamente un nivel de protección esencialmente equivalente. En particular, si el Derecho del tercer país no cumple los requisitos de las GEE, esto implicaría asegurarse de que la legislación en cuestión no incide en las garantías y salvaguardias relativas a la transferencia, con el fin de brindar en cualquier caso un nivel de protección esencialmente equivalente al garantizado en la Unión.

54. El CEPD ha emitido directrices y recomendaciones adicionales que se han de tener en cuenta para proceder a la apreciación, en función de la herramienta de transferencia utilizada y la necesidad de ofrecer unas garantías adecuadas, incluidas, en su caso, medidas complementarias.[72]

55. Por añadidura, cabe reseñar que las garantías esenciales europeas se basan en requisitos dispuestos en Derecho. El CEPD subraya que las garantías esenciales europeas se basan en los derechos fundamentales que asisten a todas las personas, con independencia de su nacionalidad.

56. El CEPD reitera que las garantías esenciales europeas son una norma de referencia para apreciar la injerencia que suponen medidas de vigilancia de terceros países, en el contexto de flujos transfronterizos de datos. Estas normas dimanan del Derecho de la Unión y la jurisprudencia del TJUE y el TEDH, vinculantes para los Estados miembros.

[71] TEDH, Kennedy, apartado 153.
[72] *Adequacy Referential*, WP 254 rev. 01, revisado y adoptado el 6 de febrero de 2018; Recomendaciones del CEPD 01/2020 sobre medidas que complementan las herramientas de transferencia para garantizar el cumplimiento del nivel de protección de datos personales de la UE, 10 de noviembre de 2020.