Edición provisional

CONCLUSIONES DEL ABOGADO GENERAL
SR. MICHAL BOBEK
presentadas el 13 de enero de 2021 (1)

Asunto C-645/19

Facebook Ireland Limited,
Facebook Inc.,
Facebook Belgium BVBA
contra
Gegevensbeschermingsautoriteit

[Petición de decisión prejudicial planteada por el hof van beroep te Brussel (Tribunal de Apelación de Bruselas, Bélgica)]

«Petición de decisión prejudicial — Protección de las personas físicas en lo que respecta al tratamiento de datos personales — Carta de los Derechos Fundamentales de la Unión Europea — Artículos 7, 8 y 47 — Reglamento (UE) 2016/679 — Artículos 55, 56, 58, 60, 61 y 66 — Autoridades de control — Tratamiento transfronterizo de datos — Ventanilla única — Autoridad de control principal — Autoridad de control interesada — Competencia — Poderes — Poder para ejercitar acciones judiciales»

I. Introducción

1. ¿Permite el Reglamento General de Protección de Datos (2) (en lo sucesivo, «RGPD») que una autoridad de control de un Estado miembro entable un procedimiento ante un tribunal de ese Estado por una presunta infracción de dicho Reglamento con respecto al tratamiento transfronterizo de datos, cuando esa autoridad *no sea la autoridad de control principal* con respecto a ese tratamiento?

2. ¿O evita exactamente que eso suceda el nuevo mecanismo de «ventanilla única», anunciado como una de las principales novedades introducidas por el RGPD? Si un responsable del tratamiento fuera llamado a defenderse frente una impugnación legal relativa al tratamiento transfronterizo de datos entablada por una autoridad de control en un tribunal ajeno al lugar del establecimiento principal del responsable, ¿sería ello una «ventanilla única excesiva» y, por tanto, incompatible con el nuevo mecanismo del RGPD?

II. Marco jurídico

A. Derecho de la Unión

3. En la exposición de motivos del RGPD se señala, entre otros extremos, que: «aunque los objetivos y principios de la Directiva 95/46/CE siguen siendo válidos, ello no ha impedido que la protección de los datos en el territorio de la Unión se aplique de manera fragmentada, [ni] la inseguridad jurídica» (considerando 9); debe garantizarse en toda la Unión que la aplicación de las normas de protección de datos sea coherente y homogénea (considerando 10); las autoridades de control deben vigilar la aplicación de las normas y contribuir a su aplicación coherente, a fin de proteger a las personas físicas y facilitar la libre circulación de datos personales en el mercado interior (considerando 123); en situaciones que conlleven un tratamiento transfronterizo, «la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado debe actuar como autoridad principal», y dicha autoridad debe «cooperar con las demás autoridades interesadas» (considerando 124).

4. A tenor del artículo 51, apartado 1, del RGPD, «cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades públicas independientes (en adelante "autoridad de control") supervisar la aplicación del presente Reglamento, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión».

5. Con arreglo a lo dispuesto en el artículo 55, apartado 1, del RGPD, «cada autoridad de control será competente para desempeñar las funciones que se le asignen y ejercer los poderes que se le confieran de conformidad con el presente Reglamento en el territorio de su Estado miembro».

6. El artículo 56 del RGPD se refiere a la competencia de la autoridad de control principal. El primer apartado de dicha disposición establece lo siguiente:

«Sin perjuicio de lo dispuesto en el artículo 55, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento será competente para actuar como autoridad de control principal para el tratamiento transfronterizo realizado por parte de dicho responsable o encargado con arreglo al procedimiento establecido en el artículo 60.»

7. Según establece el artículo 56, apartados 2 a 5, como excepción al apartado 1, «cada autoridad de control será competente para tratar una reclamación que le sea presentada o una posible infracción del presente Reglamento, en caso de que se refiera únicamente a un establecimiento situado en su Estado miembro o únicamente afecte de manera sustancial a interesados en su Estado miembro». Estos asuntos pueden ser tramitados por las autoridades de control principales, actuando según el procedimiento establecido en el artículo 60 del RGPD, o, en caso de que la autoridad de control principal decida no tratar el caso, por la autoridad de control local, actuando de conformidad con los artículos 61 y 62 del RGPD.

8. El artículo 56, apartado 6, señala que «la autoridad de control principal será el único interlocutor del responsable o del encargado en relación con el tratamiento transfronterizo realizado por dicho responsable o encargado».

9. El artículo 58, apartado 5, del RGPD, relativo a los poderes de las autoridades de control, establece lo siguiente:

«Cada Estado miembro dispondrá por ley que su autoridad de control esté facultada para poner en conocimiento de las autoridades judiciales las infracciones del presente Reglamento y, si procede, para iniciar o ejercitar de otro modo acciones judiciales, con el fin de hacer cumplir lo dispuesto en el mismo.»

10. El capítulo VII del RGPD, que lleva por título «Cooperación y coherencia», incluye los artículos 60 a 76. El artículo 60, que lleva por título «Cooperación entre la autoridad de control principal y las demás autoridades de control interesadas», establece el procedimiento detallado que deben seguir las autoridades de control principales cuando se ocupan del tratamiento transfronterizo de datos.

11. A su vez, el artículo 61, apartado 2, del RGPD, relativo a la asistencia mutua, exige que cada autoridad de control adopte «todas las medidas oportunas requeridas para responder a una solicitud de otra autoridad de control sin dilación indebida y a más tardar en el plazo de un mes a partir de la solicitud». El artículo 61, apartado 8, del RGPD, señala que cuando una autoridad de control no facilite la información solicitada, la autoridad de control requirente podrá adoptar una medida provisional en el territorio de su Estado miembro, y en ese caso se supondrá que existe la necesidad urgente contemplada en el artículo 66, apartado 1.

12. El artículo 65, apartado 1, letra a), del RGPD, que lleva por título «Resolución de conflictos por el Comité», establece que, con el fin de garantizar una aplicación correcta y coherente del Reglamento en casos concretos, el Comité Europeo de Protección de Datos (en lo sucesivo, «Comité») adoptará una decisión vinculante, entre otros, en los siguientes casos: cuando una autoridad de control interesada haya manifestado una objeción pertinente y motivada a un proyecto de decisión de la autoridad principal, o esta haya rechazado dicha objeción por no ser pertinente o no estar motivada.

13. El artículo 66, apartado 1, relativo al procedimiento de urgencia, establece que, en circunstancias excepcionales, cuando una autoridad de control interesada considere que es urgente intervenir para proteger los derechos y las libertades de interesados, podrá, como excepción a los mecanismos de coherencia, «adoptar inmediatamente medidas provisionales destinadas a producir efectos jurídicos en su propio territorio, con un período de validez determinado que no podrá ser superior a tres meses».

14. El capítulo VIII del RGPD, que lleva por título «Recursos, responsabilidad y sanciones», incluye los artículos 77 a 84. El artículo 77, apartado 1, confiere a todo interesado el derecho a presentar una reclamación ante una autoridad de control en cuanto a las posibles infracciones del Reglamento frente al tratamiento de datos personales que le conciernen, «en particular en el Estado miembro en el que tenga su residencia habitual, lugar de trabajo o lugar de la supuesta infracción». A su vez, el artículo 78, apartados 1 y 2, del RGPD confiere a toda persona física o jurídica el derecho a la tutela judicial efectiva contra, entre otras, una decisión jurídicamente vinculante de una autoridad de control que le concierna, y contra una autoridad de control que no dé curso a una reclamación.

B. Derecho nacional

15. La Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (Ley de 8 de diciembre de 1992 de protección de la intimidad en relación con el tratamiento de datos personales; en lo sucesivo, «WVP»), en su versión modificada, transpuso la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. (3) Entre otros extremos, dicha ley constituyó la Comisión para la Protección de la Privacidad belga. En virtud del artículo 32, apartado 3, de dicha ley, «sin perjuicio de la competencia de los juzgados y tribunales ordinarios para la aplicación de los principios generales de protección de la privacidad, el presidente de la [Comisión para la Protección de la Privacidad] podrá someter al juzgado de primera instancia cualquier controversia relativa a la aplicación de la presente ley y sus medidas de ejecución».

16. A tenor del artículo 3 de la Wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit (Ley de 3 de diciembre de 2017 por la que se constituye la Autoridad de Protección de Datos belga; en lo sucesivo, «Ley APD») —que entró en vigor el 25 de mayo de 2018— se constituyó una Autoridad de Protección de Datos (en lo sucesivo, «APD») para suceder a la Comisión para la Protección de la Privacidad. De conformidad con el artículo 6 de dicha ley, la APD «estará facultada para poner en conocimiento de las autoridades judiciales las violaciones de los principios básicos de protección de los datos personales, en el marco de la presente ley y de las leyes que contengan disposiciones en materia de protección del tratamiento de datos personales y, cuando proceda, para ejercitar acciones judiciales con el fin de hacer cumplir dichos principios básicos».

17. La Ley APD no incluyó ninguna disposición específica con respecto a los procesos judiciales iniciados al amparo del artículo 32, apartado 3, de la WVP que aún estaban pendientes el 25 de mayo de 2018.

18. La WVP fue derogada por la Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (Ley de 30 de julio de 2018 relativa a la protección de las personas físicas en relación con el tratamiento de datos personales). Esa ley desarrolla las disposiciones del RGPD que imponen o permiten a los Estados miembros adoptar reglas más detalladas, además de las reglas comunes.

III. Hechos, procedimiento nacional y cuestiones prejudiciales

19. El 11 de septiembre de 2015, el presidente de la Comisión para la Protección de la Privacidad de Bélgica, que posteriormente se convirtió en la APD, inició un procedimiento contra Facebook Inc., Facebook Ireland Ltd. y Facebook BVBA (en lo sucesivo, conjuntamente, «Facebook») ante el Nederlandstalige rechtbank van eerste aanleg Brussel (Tribunal de Primera Instancia Neerlandófono de Bruselas, Bélgica). Dicho procedimiento se refiere a presuntas infracciones de las leyes de protección de datos por parte de Facebook, consistentes, entre otras cosas, en recoger y utilizar de forma ilícita información sobre los hábitos de navegación privados de los usuarios de Internet en Bélgica por medio de tecnologías tales como *cookies*, *social plug-ins* (complementos sociales) y «píxeles».

20. De forma resumida, la APD alega que Facebook utiliza determinadas tecnologías diseñadas para la vigilancia y el seguimiento de las personas mientras navegan de un sitio web a otro y, a continuación, utiliza la información recogida para perfilar sus hábitos de navegación y, sobre tal base, les muestra publicidad personalizada, sin informar debidamente a los afectados y sin obtener su consentimiento válido. La APD sostiene que Facebook aplica estas prácticas con independencia de si el afectado se ha hecho o no miembro de la red social de Facebook.

21. La APD solicitó que se ordenara a Facebook que, con respecto a cualquier usuario de Internet establecido en el territorio belga, dejase de insertar, sin su consentimiento, *cookies* que permanecen activas durante dos años en los dispositivos que utilizan esas personas cuando navegan por una página web en el dominio Facebook.com o en un sitio web de un tercero, así como que dejase de recopilar datos, de forma excesiva, mediante *social plug-ins* y píxeles en sitios web de terceros. Además, solicitó la destrucción de todos los datos personales obtenidos mediante *cookies* y *social plug-ins* relativos a cada usuario de Internet establecido en el territorio belga.

22. Mediante auto de medidas cautelares de 9 de noviembre de 2015, el presidente del Nederlandstalige rechtbank van eerste aanleg Brussel (Tribunal de Primera Instancia Neerlandófono de Bruselas) declaró que tenía competencia para conocer del asunto y que la demanda era admisible con respecto a las tres demandadas. Asimismo, dicho tribunal ordenó a las demandadas el cese provisional de determinadas actividades en relación con los usuarios de Internet situados en el territorio belga.

23. El 2 de marzo de 2016, Facebook interpuso un recurso de apelación contra ese auto ante el hof van beroep te Brussel (Tribunal de Apelación de Bruselas, Bélgica). Mediante sentencia de 29 de junio de 2016, dicho tribunal modificó el auto de primera instancia. En particular, dicho tribunal dictaminó que carecía de competencia con respecto a las acciones contra Facebook Inc. y Facebook Ireland Ltd, mientras que sí tenía competencia con respecto a la acción ejercitada contra Facebook Belgium BVBA. Por tanto, el procedimiento principal quedó restringido a la pretensión formulada contra Facebook Belgium BVBA. Dicho tribunal también declaró que el asunto no tenía carácter urgente.

24. Entiendo que, en la actualidad, el asunto pendiente ante el hof van beroep te Brussel (Tribunal de Apelación de Bruselas) se refiere al recurso de apelación interpuesto contra una resolución posterior sobre el fondo dictada por el tribunal de primera instancia. En el seno del procedimiento de apelación, Facebook Belgium sostiene, entre otros extremos, que desde que el nuevo mecanismo de «ventanilla única» del

RGPD comenzó a ser aplicable, la APD perdió la competencia para continuar el procedimiento principal porque no es la autoridad de control principal. Por lo que respecta al tratamiento transfronterizo que nos ocupa, la autoridad de control principal sería la Data Protection Commission irlandesa. El establecimiento principal del responsable del tratamiento en la Unión Europea se encuentra en Irlanda (Facebook Ireland Ltd).

25. En este contexto, el hof van beroep te Brussel (Tribunal de Apelación de Bruselas) decidió suspender el procedimiento y plantear al Tribunal de Justicia las siguientes cuestiones prejudiciales:

«1) ¿Deben interpretarse los artículos [55, apartado 1], 56 a 58 y 60 a 66 del [RGPD], en relación con los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea, en el sentido de que una autoridad de control que, en virtud de la legislación nacional adoptada en ejecución del artículo [58, apartado 5], de dicho Reglamento, está facultada para iniciar acciones judiciales contra infracciones de este Reglamento ante un tribunal de su Estado miembro, no puede ejercitar tal facultad en relación con un tratamiento transfronterizo si no es la autoridad de control principal en materia de tratamiento transfronterizo?

2) ¿Tiene alguna incidencia en la respuesta a la anterior cuestión prejudicial si el responsable del tratamiento transfronterizo no tiene su establecimiento principal en ese Estado miembro, pero sí tiene otro establecimiento en el mismo?

3) ¿Tiene alguna incidencia en la respuesta a la primera cuestión prejudicial si la autoridad de control nacional inicia la acción judicial contra el establecimiento principal del responsable del tratamiento o contra el establecimiento en su propio Estado miembro?

4) ¿Tiene alguna incidencia en la respuesta a la primera cuestión prejudicial si la autoridad de control nacional ya inició acciones judiciales antes de la fecha en que este Reglamento resultó aplicable (25 de mayo de 2018)?

5) En caso de respuesta afirmativa a la primera cuestión prejudicial, ¿tiene efecto directo el artículo [58, apartado 5], del RGPD, de modo que una autoridad de control nacional podrá invocar el citado artículo para iniciar o continuar un procedimiento judicial contra particulares, aun cuando el artículo [58, apartado 5], del RGPD no haya sido transpuesto específicamente a la legislación de los Estados miembros, pese a que se exige tal transposición?

6) En caso de respuesta afirmativa a las anteriores cuestiones prejudiciales, ¿se opondría el resultado de tales procedimientos que la autoridad de control principal llegase a la conclusión contraria en el caso de que dicha autoridad de control principal investigase las mismas actividades de tratamiento transfronterizo u otras similares de conformidad con el mecanismo establecido en los artículos 56 y 60 del RGPD?»

26. Han presentado observaciones escritas Facebook, la APD, los Gobiernos belga, checo, italiano, polaco, portugués y finlandés, así como la Comisión Europea. Facebook, la APD y la Comisión formularon asimismo observaciones orales en la vista celebrada el 5 de octubre de 2020.

IV. Análisis

27. En pocas palabras, la cuestión clave que surgió en el procedimiento principal es si la APD puede continuar un procedimiento judicial contra Facebook Belgium con respecto al tratamiento transfronterizo de datos personales que tuvo lugar después de que el RGPD comenzara a ser aplicable, dado que la entidad encargada del tratamiento de los datos es Facebook Ireland Ltd.

28. Para abordar esta cuestión, es necesario evaluar el alcance y el funcionamiento de lo que el propio RGPD, en el considerando 127, denomina el mecanismo de «ventanilla única». Dicho mecanismo consiste

en un conjunto de normas que dan lugar, en el caso del tratamiento transfronterizo de datos, a un punto central de ejecución a través de una *autoridad de control principal* (en lo sucesivo, «ACP»), integrada en el sistema de procedimientos de cooperación y coherencia junto con las *autoridades de control interesadas* (en lo sucesivo, «ACI»), diseñado para garantizar la participación de todas las autoridades de control interesadas.

29. A tenor del artículo 56, apartado 1, del RGPD, la autoridad de control actúa como ACP con respecto al tratamiento transfronterizo realizado por los responsables o los encargados del tratamiento que tengan su establecimiento principal o el único establecimiento en su territorio. Según el artículo 4, apartado 22, del RGPD, una autoridad de control actúa como ACI si se satisface una de las siguientes condiciones alternativas: «a) el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control; b) los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento; o c) se ha presentado una reclamación ante esa autoridad de control».

30. Antes de abordar el fondo de las cuestiones prejudiciales planteadas, se precisan algunas observaciones preliminares (A). Pasaré luego al examen de las cuestiones jurídicas planteadas por el tribunal remitente. Haré hincapié, en particular, en la primera cuestión prejudicial planteada, ya que se encuentra en el centro del litigio sustanciado ante el tribunal remitente (B). A continuación, me ocuparé de las otras cuestiones planteadas solo brevemente, dado que, si la respuesta a la primera cuestión prejudicial es la que se propone en las presentes conclusiones, la respuesta a esas otras cuestiones se vuelve innecesaria o bastante sencilla (C).

A. Observaciones preliminares

31. De entrada, observo que hay determinados elementos del procedimiento principal que me cuesta comprender plenamente.

32. En primer lugar, debo admitir que la pertinencia de las cuestiones planteadas en el curso del procedimiento principal no me resulta del todo obvia, dado que, de todas las partes frente a las que la APD dirigió su demanda, parece ser que solo Facebook Belgium sigue siendo parte demandada en el procedimiento principal. (4) De los autos a disposición del Tribunal de Justicia se desprende que dicha empresa no es el «establecimiento principal» del responsable del tratamiento a efectos del artículo 4, apartado 16, del RGPD, ni, puesto que parece ser un establecimiento de la misma empresa, potencialmente un «corresponsable del tratamiento» en el sentido del artículo 26 del RGPD. (5)

33. No obstante, las cuestiones que se plantean en el marco de una petición de decisión prejudicial gozan de presunción de pertinencia. Por ello, el Tribunal de Justicia se niega a pronunciarse solo en circunstancias limitadas, en particular, cuando no se cumplen los requisitos del artículo 94 del Reglamento de Procedimiento del Tribunal de Justicia o cuando es obvio que la interpretación del Derecho de la Unión en cuestión no guarda relación alguna con los hechos, o cuando las cuestiones son (completamente) hipotéticas. (6) A mi juicio, eso no ocurre en el presente asunto. Dilucidar «quién es quién» y «contra quién se puede entablar un procedimiento determinado» no es solo una apreciación fáctica que, en última instancia, incumbe al órgano jurisdiccional nacional, sino que es también, en cierto modo, uno de los extremos de las cuestiones planteadas al Tribunal de Justicia.

34. En segundo lugar, el aspecto de la temporalidad del procedimiento principal tampoco resulta fácil de comprender del todo. La acción se ejerció mientras estaba en vigor la Directiva 95/46. Posteriormente se mantuvo cuando entró en vigor el RGPD. No obstante, el procedimiento aparentemente solo se refiere ahora a conductas desarrolladas *después* de que comenzara a ser aplicable el nuevo marco legal. De hecho, se plantea el problema de si la continuación del procedimiento por parte de la APD es coherente con las disposiciones del RGPD, un elemento que pone de manifiesto la cuarta pregunta. No obstante, estas cuestiones solo serían pertinentes en el procedimiento principal si una autoridad nacional quisiera dar por concluido el procedimiento en curso con respecto a las presuntas infracciones anteriores al momento en que el nuevo marco legal comenzó a ser aplicable. Sin embargo, si el procedimiento en curso en este

momento se refiriese únicamente a la presunta ilegalidad que tuvo lugar después de la fecha en la que el RGPD comenzó a ser aplicable, probablemente junto con la solicitud de la prohibición judicial (necesariamente prospectiva) de tales prácticas, no es fácil de entender por qué la APD, en la medida en que se considera competente para intervenir, no puso fin al procedimiento actual y no procedió al amparo de las disposiciones pertinentes del RGPD.

35. En tercer lugar, en la vista, la APD se refirió a un intercambio de comunicaciones que tuvo con la autoridad de control irlandesa y el Comité sobre una de las tecnologías utilizadas por Facebook para recopilar datos (*cookies*). Se ha afirmado que las dos autoridades de control discreparon sobre si esa tecnología realmente estaba incluida en el ámbito de aplicación *ratione materiae* del RGPD.

36. A este respecto, y por lo que se refiere al presente asunto, cabe señalar que determinadas actividades de tratamiento de datos pueden estar comprendidas efectivamente en el ámbito de aplicación material de más de un instrumento legislativo de la Unión, en cuyo caso todos esos instrumentos, salvo que se disponga lo contrario, son aplicables al mismo tiempo. (7) No obstante, en otros casos, por ejemplo, cuando las actividades de tratamiento no afectan a datos *personales* en el sentido del artículo 4, apartado 1, del RGPD, obviamente no se aplica el RGPD.

37. En consecuencia, cuando la presunta ilegalidad de algunos tipos de tratamiento de datos dimana de otras disposiciones del Derecho (de la Unión o nacional), no entran en juego los procedimientos y mecanismos establecidos en el RGPD. El RGPD no puede utilizarse como pasarela para incorporar al mecanismo de «ventanilla única» formas de conducta que, aunque conlleven algunos flujos de datos o incluso su tratamiento, no incumplan ninguna de las obligaciones establecidas en aquel.

38. Para decidir si un asunto se encuentra o no dentro del ámbito de aplicación del RGPD *ratione materiae*, cualquier tribunal nacional, lo que incluye a cualquier tribunal remitente, debe investigar la *fuente exacta de la obligación legal* que incumbe a un operador económico y que supuestamente ha sido infringida por este último. Si la fuente de esa obligación no es el RGPD, entonces los procedimientos establecidos por ese instrumento, vinculados al ámbito sustantivo de este, lógicamente tampoco son aplicables.

B. Sobre la primera cuestión prejudicial

39. Mediante su primera cuestión prejudicial, el tribunal remitente pregunta esencialmente si las disposiciones del RGPD, examinadas a la luz de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»), permiten que la autoridad de control de un Estado miembro entable un procedimiento ante un tribunal de ese Estado por una presunta infracción del RGPD con respecto al tratamiento transfronterizo de datos, aunque esa autoridad no sea la «autoridad de control principal».

40. A este respecto, la APD y los Gobiernos belga, italiano, polaco y portugués proponen que el Tribunal de Justicia responda afirmativamente, mientras que Facebook, los Gobiernos checo y finlandés, así como la Comisión, adoptan la postura contraria.

41. A continuación, explicaré por qué no encuentro convincente la interpretación del RGPD propuesta por la APD y los Gobiernos belga, italiano, polaco y portugués: una interpretación tanto literal y sistemática (1), como teleológica e histórica (2) del RGPD apunta claramente en la dirección opuesta. Además, ni una interpretación del Reglamento orientada a la Carta (3), ni los supuestos riesgos de la posible falta de aplicación del RGPD (4) son tales como para poner en cuestión lo que, a mi juicio, es la interpretación adecuada del RGPD, ciertamente no en este momento.

42. Dicho esto, las consecuencias de esa lectura particular del Reglamento no son, a mi juicio, tan extremas como las sugeridas por Facebook, los Gobiernos checo y finlandés y la Comisión. Por consiguiente, explicaré por qué la respuesta que debe darse al tribunal remitente debe situarse en un término medio entre las dos posiciones planteadas en este procedimiento: la autoridad de control de un

Estado miembro *está* facultada para entablar un procedimiento ante un tribunal de ese Estado por una presunta infracción del RGPD con respecto al tratamiento transfronterizo de datos, pese a no ser la ACP, *siempre* que lo haga en las situaciones y según los procedimientos establecidos en el RGPD (5).

1. Una interpretación literal y sistemática del RGPD

43. En primer lugar, me parece que la redacción de las disposiciones pertinentes, especialmente cuando se leen en su contexto, abona la interpretación del RGPD según la cual la ACP tiene una competencia general sobre el tratamiento transfronterizo e, implícitamente, las ACI disfrutan de un poder limitado para actuar a ese respecto.

44. El artículo 56, apartado 1, del RGPD dispone que «la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento *será competente para actuar como autoridad de control principal para el tratamiento transfronterizo* realizado por parte de dicho responsable o encargado con arreglo al procedimiento establecido en el artículo 60». (8) Según el artículo 56, apartado 6, del RGPD, «la autoridad de control principal *será el único interlocutor* del responsable o del encargado en relación con el tratamiento transfronterizo realizado por dicho responsable o encargado». (9) El considerando 124 se hace eco de dichas disposiciones, señalando esencialmente que, en el caso del tratamiento transfronterizo, «la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado *debe actuar como autoridad principal*». (10)

45. La competencia general de la ACP sobre el tratamiento transfronterizo de datos se ve confirmada además por el hecho de que las situaciones en las que la competencia con respecto al tratamiento transfronterizo se confiere a otras autoridades de control se describen como *excepciones* a la regla general. En particular, el artículo 55, apartado 2, del RGPD excluye la competencia de la ACP sobre determinado tratamiento de datos «efectuado por autoridades públicas». Además, el artículo 56, apartado 2, del RGPD, establece que, como excepción al principio de que la competencia corresponde a la ACP, «cada autoridad de control será competente para tratar una reclamación que le sea presentada o una posible infracción del presente Reglamento, en caso de que se refiera únicamente a un establecimiento situado en su Estado miembro o únicamente afecte de manera sustancial a interesados en su Estado miembro».

46. Por otra parte, el artículo 66 del RGPD, que regula el «procedimiento de urgencia», faculta a cada ACI «en circunstancias excepcionales», cuando haya una necesidad urgente de intervenir para proteger los derechos y las libertades de interesados, para adoptar inmediatamente medidas provisionales destinadas a producir efectos jurídicos en su propio territorio, con un período de validez determinado que no podrá ser superior a tres meses, «como excepción» a los mecanismos de cooperación y coherencia contemplados en los artículos 60, 63, 64 y 65 del RGPD.

47. Por lo tanto, me parece bastante claro a partir del texto del RGPD que, en relación con el tratamiento transfronterizo, la competencia de la ACP es la regla y la competencia de otras autoridades de control es la excepción. (11)

48. No obstante, la APD y ciertos gobiernos cuestionan esa lectura del RGPD. En su opinión, el texto de las disposiciones pertinentes sugiere un derecho (casi ilimitado) de cualquier autoridad de control a entablar procedimientos judiciales contra posibles infracciones que afecten a sus territorios, independientemente de que el tratamiento tenga carácter transfronterizo. Esgrimen principalmente dos argumentos.

49. En primer lugar, argumentan que la expresión «sin perjuicio de lo dispuesto en el artículo 55», con la que comienza el artículo 56, apartado 1, significa que la competencia otorgada a la ACP por esta última disposición no puede menoscabar ni limitar los poderes atribuidos por la primera disposición a *cada* autoridad de control, incluido el de iniciar procedimientos judiciales.

50. Este argumento no me convence.

51. El artículo 55, apartado 1, establece el principio según el cual «cada autoridad de control será competente para desempeñar las funciones que se le asignen y ejercer los poderes que se le confieran de conformidad con el presente Reglamento en el territorio de su Estado miembro». A continuación, esas funciones se relacionan en el artículo 57 del RGPD. Los poderes se relacionan en el artículo 58 del mismo. Entre las funciones asignadas se encuentra concretamente la de controlar la aplicación del RGPD y hacerlo aplicar [artículo 57, apartado 1, letra a)]. Los poderes que se otorgan en virtud del artículo 58 incluyen diversos poderes de investigación (apartado 1), correctivos (apartado 2), de autorización y consultivos (apartado 3), así como el poder de ejercitar acciones judiciales (apartado 5).

52. En esencia, esas disposiciones —a las que se refiere tácitamente el artículo 55— abarcan *todas* las funciones y poderes conferidos a las autoridades de control en virtud del RGPD. Si se siguiera la interpretación planteada por la APD y ciertos gobiernos, prácticamente no quedaría nada para la competencia general de la ACP, privando así al artículo 56 de todo sentido. La ACP no sería el «único» interlocutor, ni tendría ningún carácter «principal» con respecto a las demás autoridades de control en modo alguno. Podría decirse que su función se reduciría a la de un «punto informativo» sin una misión claramente definida.

53. La importancia de la función conferida a la ACP, e implícitamente del mecanismo de ventanilla única, emerge aún más específicamente cuando se leen todas esas disposiciones juntas y contextualmente.

54. La prominencia que se le da al artículo 56 dentro del esquema del RGPD es un primer indicio de ello. El artículo 56 es la segunda disposición que figura en la sección pertinente del RGPD (capítulo VI, «Autoridades de control independientes», Sección 2, «Competencia, funciones y poderes») y se sitúa inmediatamente después de la disposición general sobre «competencia» y antes de las otras disposiciones generales sobre «funciones» y «poderes». Por lo tanto, el legislador de la Unión ha decidido hacer hincapié en la centralidad de la competencia de la ACP incluso antes de pasar a detallar las funciones y poderes específicos de *todas* las autoridades de control.

55. Pero, fundamentalmente, la importancia de la función de la ACP también se ve confirmada por las disposiciones incluidas en el capítulo VII del RGPD (que lleva por título «Cooperación y coherencia»), que establece los diversos procedimientos y mecanismos que las autoridades de control deben seguir para garantizar la aplicación coherente del RGPD. En particular, el artículo 60, que da comienzo al capítulo y al que se refiere el artículo 56, apartado 1, establece el procedimiento de «cooperación entre la autoridad de control principal y las demás autoridades de control interesadas».

56. Está claro que se pretende que ese sea *el* procedimiento que debe seguirse cuando sea necesaria una acción por incumplimiento en casos de tratamiento transfronterizo. Ese procedimiento, al igual que sucede con los demás procedimientos previstos en el capítulo VII del RGPD, no es opcional. Los términos imperativos incluidos, en particular en el artículo 51, apartado 2, y el artículo 63 del RGPD, indican inequívocamente que las autoridades de control deben cooperar y deben hacerlo mediante el uso (obligatorio) de los procedimientos y mecanismos establecidos para tal fin.

57. Por tanto, la expresión «sin perjuicio de lo dispuesto en el artículo 55», contenida en el artículo 56, apartado 1, tiene un significado diferente al sugerido por la APD. A mi juicio, esa frase, en el contexto en el que se sitúa, simplemente significa que incluso si en un asunto individual es la ACP la que resulta *competente* para ese asunto en materia de tratamiento transfronterizo conforme al artículo 56 del RGPD, todas las autoridades de control conservan naturalmente los *poderes* generales que se les asignan en virtud del artículo 55 (y el artículo 58) del RGPD.

58. A tenor del artículo 55, apartado 1, del RGPD, los Estados miembros deben permitir que la autoridad de control desempeñe las funciones y ejerza los poderes previstos en el Reglamento. Por lo tanto, esa disposición asigna a cualquier autoridad de control un poder (o competencia) general para actuar con respecto a su territorio, y eso sigue siendo cierto independientemente («*sin perjuicio*») de que el tratamiento tenga carácter transfronterizo o no y, si efectivamente lo es, la autoridad en cuestión actúa como la ACP o la ACI. (12) No obstante, el artículo 55 del RGPD no regula las situaciones y la forma en

que se ejercerá ese poder para actuar en un caso concreto. En efecto, esos aspectos se regulan en otras disposiciones del RGPD, especialmente las incluidas en el capítulo VII del mismo. Con arreglo a dichas disposiciones, el que una autoridad de control pueda ejercer el poder general de actuar y la manera en que lo haga dependen, entre otros factores, de si, con respecto a un determinado responsable o encargado del tratamiento, esa autoridad es la ACP o la ACI. (13)

59. En este sentido y en cuanto al resultado, por lo tanto, comparto el criterio del Comité, el cual, en un reciente dictamen, se refirió al artículo 56, apartado 1, del RGPD como una «excepción» y como una «*lex specialis*»: dicho artículo «prevalece [sobre la regla general del artículo 55 del RGPD] en todos aquellos casos en que una situación de tratamiento de datos cumpla las condiciones especificadas en el mismo». (14)

60. En consecuencia, considero que la APD y ciertos gobiernos malinterpretan los artículos 55 y 56, apartado 1, del RGPD. Estas partes coadyuvantes sacan de su contexto la primera parte de la frase del artículo 56, apartado 1, a fin de invertir la relación entre la regla y la excepción. Hacerlo da como resultado la dilución del contenido prescriptivo de varias disposiciones del RGPD y frustra el objetivo, subrayado, entre otros, en el considerando 10 del mismo, de garantizar una aplicación más coherente y homogénea de las normas de protección de datos. Ello supondría esencialmente volver al régimen anterior de la Directiva 95/46.

61. En segundo lugar, la APD y algunos gobiernos sostienen que de la redacción misma del artículo 58, apartado 5, del RGPD se desprende que *todas* las autoridades de control deben poder iniciar acciones judiciales contra *cualquier* posible infracción de las normas de protección de datos que afecten a su territorio, independientemente de la naturaleza (local o transfronteriza) del tratamiento. La consecuencia es que —en su opinión— incluso si se interpretara que el mecanismo de ventanilla única limita los poderes de otras autoridades de control con respecto al tratamiento transfronterizo, esos límites solo pueden afectar a la acción administrativa y no al procedimiento judicial.

62. Este segundo argumento también resulta, a mi juicio, insostenible. Comete el mismo «pecado» del argumento anterior: leer una disposición específica del RGPD en «aislamiento clínico» del resto del Reglamento y, al mismo tiempo, darle una importancia excesiva.

63. El artículo 58, apartado 5, del RGPD establece que «cada Estado miembro dispondrá por ley que su autoridad de control esté facultada para poner en conocimiento de las autoridades judiciales las infracciones del presente Reglamento y, si procede, para iniciar o ejercitar de otro modo acciones judiciales, con el fin de hacer cumplir lo dispuesto en el mismo».

64. Esta disposición obliga a los Estados miembros, por un lado, a permitir que las autoridades de control mantengan vínculos estrechos con las autoridades judiciales (incluidas potencialmente las autoridades penales) y, por otro lado, a otorgar a las autoridades de control una legitimación (no solo pasiva sino también activa) ante sus juzgados y tribunales nacionales. Dicho de otra manera, las autoridades de control deberían, en principio, ser capaces de interactuar con las autoridades judiciales y, si es necesario, iniciar procedimientos judiciales. Entiendo que el legislador de la Unión consideró necesaria una disposición expresa de este tipo ya que, pese al texto del artículo 28, apartado 3, de la Directiva 95/46, (15) existían diferencias significativas entre las legislaciones de los Estados miembros sobre este asunto, lo que a su vez creaba problemas de incumplimiento. (16) El presente asunto, iniciado cuando dicha Directiva aún estaba en vigor, ofrece un ejemplo al respecto: el asunto planteó, con arreglo al Derecho nacional, problemas de legitimación de la Comisión para la Protección de la Privacidad y de adecuación del fundamento jurídico de la acción entablada por su presidente.

65. No obstante, de manera similar a lo que ya se ha señalado anteriormente, (17) el artículo 58, apartado 5, del RGPD establece *poderes* que deben otorgarse a todas las autoridades de control sin excepciones en esa etapa, independientemente de (o antes de) la determinación, en un asunto individual, de si esa autoridad sería la ACP *competente*, la ACI o potencialmente una autoridad no interesada en absoluto. El artículo 58, apartado 5, del RGPD no regula las situaciones ni la manera en que debe ejercerse

ese poder de entablar acciones judiciales. Presumiblemente, esta es también la razón por la que esa disposición incluye la expresión «si procede». Ese es el objeto de otras disposiciones del RGPD.

66. Además, ni el texto ni la estructura del artículo 58 del RGPD sugieren que se pueda trazar una distinción —como sostiene la APD— entre los *poderes administrativos* de las autoridades (que estarían sujetos a las limitaciones dimanantes del mecanismo de ventanilla única) y el *poder para ejercitar acciones judiciales* (que no estaría sujeto a dichas limitaciones). Dicha disposición relaciona, apartado tras apartado, los diversos poderes que deben otorgarse a las autoridades de control, agrupándolos por finalidad (de investigación, correctiva, consultiva, etc.). La redacción de esos apartados es bastante similar y, en esencia, indica que *cada* autoridad de control tendrá los poderes que allí se establecen.

67. Por lo tanto, no veo motivo alguno para interpretar el apartado 5 del artículo 58 de manera diferente a los apartados 1 a 3 de la misma disposición. De las dos tesis, solo una puede ser cierta: o todas y cada una de las autoridades de control disfrutan de todos esos poderes sin que se vean restringidos por el mecanismo de ventanilla única, o todos esos poderes deben ejercerse con arreglo a los procedimientos y dentro de los límites establecidos en el Reglamento.

68. Por las razones explicadas en los puntos 51 y 52 anteriores, la primera hipótesis no puede sostenerse. En realidad, cuando se lee el artículo 58 del RGPD en su contexto, queda claro que, en todo caso, lo realmente cierto es lo contrario de lo que afirman la APD y algunos gobiernos.

69. De hecho, cada autoridad de control debe contribuir a la aplicación correcta y coherente del Reglamento. A tal fin, cada autoridad de control —independientemente de su función como ACP o como ACI en un asunto específico— debe, por ejemplo, examinar las reclamaciones que se le presenten y hacerlo con la debida diligencia. (18) En efecto, incluso cuando las presuntas infracciones se refieran a un tratamiento transfronterizo y una autoridad no sea la ACP, otras autoridades de control deberían ser capaces de examinar el asunto a fin de proporcionar una aportación significativa cuando se les solicite en el marco de los mecanismos de cooperación y coherencia, (19) o adoptar medidas urgentes. No obstante, corresponde entonces a la ACP, con carácter general, adoptar decisiones vinculantes para hacer cumplir el RGPD frente al encargado o al responsable del tratamiento. (20) En particular, como se desprende de la reciente sentencia dictada en el asunto Facebook Ireland y Schrems, incumbe a «la autoridad nacional de control *competente* […] en su caso, interponer un recurso ante los tribunales nacionales». (21) Por tanto, la sugerencia de que las autoridades de control puedan pasar por alto los mecanismos de coherencia y cooperación cuando deseen ejercitar acciones judiciales no puede conciliarse con el texto del RGPD y la jurisprudencia del Tribunal de Justicia.

70. Además, desde una perspectiva más práctica, sería ilógico impedir que una autoridad incoe un procedimiento administrativo, con el fin de analizar el presunto incumplimiento de las normas de protección de datos con los operadores interesados, pero permitir que dicha autoridad entable inmediatamente un procedimiento judicial ante un tribunal sobre el mismo asunto. El proceso judicial es a menudo un instrumento de último recurso, que probablemente empleará una autoridad cuando un problema no pueda tratarse de manera efectiva mediante conversaciones (formales o informales) y decisiones adoptadas a nivel administrativo.

71. La distinción sugerida por la APD, que *no permitiría* a una autoridad de control (*en vía administrativa*) investigar, preparar, tramitar y decidir, pero que en cambio le *permitiría demandar* de inmediato ante un tribunal, se acerca peligrosamente a convertir a las autoridades administrativas en personajes ciertamente cuestionables de las películas del Oeste, que disparan primero, y (quizás) hablan después, si es que lo hacen («cuando tengas que disparar, dispara, no hables» (22)). No estoy seguro de que esa sea una forma razonable o apropiada de que las autoridades administrativas se ocupen de las presuntas infracciones de las normas de protección de datos.

72. Además, y lo que es más importante, permitir que las autoridades de control comparezcan libremente ante sus tribunales nacionales, cuando no puedan ejercer sus poderes administrativos sin pasar por los mecanismos de cooperación y coherencia establecidos en el Reglamento, allanaría el camino para

una fácil elusión de esos mecanismos. En particular, en caso de desacuerdo sobre un proyecto de decisión, tanto la ACP como (cada una de) las ACI podrían «tomarse la justicia por su mano» e iniciar procedimientos ante los tribunales nacionales, sorteando así el procedimiento previsto en el artículo 60, apartado 4, y el artículo 65 del RGPD.

73. Ello, a su vez, también dejaría sin sentido una de las principales funciones del Comité, un organismo establecido por el RGPD, compuesto por el director de una autoridad de control de cada Estado miembro y por el Supervisor Europeo de Protección de Datos. (23) Una de las funciones del Comité es precisamente la de supervisar y garantizar la correcta aplicación del RGPD cuando surja un desacuerdo entre diferentes autoridades de control. (24) En esos casos, el Comité actúa como foro de solución de controversias y órgano de toma de decisiones. Si se siguiera la interpretación defendida por la APD y algunos gobiernos, el mecanismo establecido en el artículo 65 del RGPD podría quedar completamente al margen: cada autoridad podría seguir su propio camino, soslayando al Comité.

74. La situación resultante parecería ser la opuesta a lo que el legislador de la Unión pretendió lograr con el nuevo sistema, como se explicará en la siguiente sección.

2. Una interpretación teleológica e histórica del RGPD

75. Como se desprende del considerando 9 del RGPD, el legislador de la Unión consideró que, si bien «los objetivos y principios de la Directiva 95/46 [seguían siendo] válidos», ese instrumento no había «impedido que la protección de los datos en el territorio de la Unión se [aplicase] de manera fragmentada, ni la inseguridad jurídica ni una percepción generalizada entre la opinión pública de que [existían] riesgos importantes para la protección de las personas físicas».

76. La necesidad de garantizar la coherencia se convirtió así en la «consigna» del instrumento jurídico destinado a sustituir a la Directiva 95/46. Este objetivo se consideró importante desde una doble perspectiva: por un lado, para garantizar un nivel homogéneo y elevado de protección de las personas físicas, y por otro, para eliminar los obstáculos a la circulación de datos personales dentro de la Unión, proporcionando seguridad jurídica y transparencia a los operadores económicos. (25)

77. Cabe destacar este último aspecto. En virtud de la Directiva 95/46, los operadores económicos activos en toda la Unión Europea estaban obligados a cumplir una serie de diferentes normas nacionales de transposición de la Directiva y, al mismo tiempo, interactuar con todas las autoridades nacionales de protección de datos. Esa situación no solo era costosa, onerosa y lenta para los operadores económicos, sino también una fuente inevitable de incertidumbre y de conflictos para esos operadores y sus clientes. (26)

78. Los límites del sistema establecido con la Directiva 95/46 también se evidenciaron en varias sentencias del Tribunal de Justicia. En Weltimmo, el Tribunal de Justicia sostuvo que los poderes de las autoridades de protección de datos estaban estrictamente limitados por el principio de territorialidad: dichas autoridades solo podían actuar contra los incumplimientos que tuvieran lugar dentro de su propio territorio, teniendo en todos los demás casos que instar la intervención de las autoridades de los demás Estados miembros. (27) En Wirtschaftsakademie Schleswig-Holstein, el Tribunal de Justicia dictaminó que, en caso de tratamiento transfronterizo, cada autoridad de protección de datos podría ejercer sus poderes con respecto a una entidad establecida en su territorio, independientemente de los criterios y acciones de la autoridad de protección de datos del Estado miembro donde tenga su domicilio la entidad responsable de dicho tratamiento. (28)

79. No obstante, en el mundo virtual del tratamiento de datos, dividir la competencia de las distintas autoridades a lo largo de líneas territoriales resulta a menudo problemático. (29) Además, la falta de mecanismos claros de coordinación entre las autoridades nacionales daba pie a incoherencias e incertidumbre.

80. La introducción del mecanismo de ventanilla única, con el papel preeminente otorgado a la ACP y los mecanismos de cooperación establecidos para hacer partícipes a otras autoridades de control, estaba destinada, por tanto, a abordar esos mismos problemas. (30) En el asunto Google (Alcance territorial del derecho a la retirada de enlaces), el Tribunal de Justicia destacó la importancia de los mecanismos de cooperación y coherencia, para la correcta y coherente aplicación del RGPD, y su carácter obligatorio. (31) Más recientemente, en el asunto Facebook Ireland y Schrems, el Abogado General Saugmandsgaard Øe también subrayó que los mecanismos de cooperación y coherencia previstos en el capítulo VII del RGPD están destinados a evitar el riesgo de que varias autoridades de control adopten enfoques diferentes con respecto al tratamiento transfronterizo. (32)

81. Es cierto que —como señala la APD— durante el proceso legislativo, tanto el Consejo como el Parlamento trataron de limitar la competencia de la ACP prevista inicialmente por la Comisión. No obstante, los cambios finalmente introducidos en el texto final del RGPD no arrojan dudas sobre la interpretación del Reglamento ilustrada anteriormente, sino que más bien la confirman.

82. Según la propuesta original de la Comisión, el mecanismo de ventanilla única implicaba que, con respecto al tratamiento transfronterizo, una sola autoridad de control (la ACP) tenía que ser responsable de supervisar las actividades del responsable o del encargado del tratamiento en toda la Unión Europea y de tomar las decisiones pertinentes. (33) No obstante, esta propuesta dio lugar a debates en el seno del Consejo y del Parlamento.

83. El Consejo finalmente pactó un texto sobre la base de una propuesta presentada por la Presidencia. (34) Esa propuesta no cuestionaba en modo alguno el mecanismo de ventanilla única como tal, que el Consejo calificó como «uno de los pilares centrales» del nuevo marco jurídico. (35) La propuesta de la Presidencia se tradujo a la postre en dos conjuntos de enmiendas bastante específicas.

84. En primer lugar, el Consejo quiso introducir determinadas *excepciones* a la competencia general de la ACP: en lo que respecta al tratamiento realizado por las autoridades públicas y en relación con las situaciones locales. Por tanto, el Consejo propuso introducir dos disposiciones que no figuraban en la propuesta de la Comisión, (36) y que son ahora el artículo 55, apartado 2, y el artículo 56, apartado 2, del RGPD. (37)

85. En segundo lugar, el Consejo pretendía *suavizar* el papel y la competencia de la ACP, haciendo que el procedimiento fuera más inclusivo. Se consideró que el texto de la propuesta de la Comisión resultaba algo ambiguo al respecto y que posiblemente daría lugar a una competencia exclusiva de la ACP sobre el tratamiento transfronterizo de datos. Por lo tanto, se introdujeron algunas correcciones en el texto a fin de reforzar la «proximidad» entre los interesados y las autoridades de control. (38) Entre otros extremos, se potenció significativamente la participación de otras autoridades de control en el proceso de toma de decisiones.

86. Por su parte, el Parlamento Europeo también apoyó la creación del mecanismo de ventanilla única, con un papel reforzado para la ACP, pero propuso fortalecer el sistema de cooperación entre las autoridades de control. Tanto la Exposición de Motivos del Proyecto de Informe del Parlamento (39) como la Resolución Legislativa del Parlamento Europeo de 12 de marzo de 2014 (40) son bastante claros en ese sentido.

87. En esencia, con la intervención del Consejo y del Parlamento, el mecanismo de ventanilla única, que anteriormente se inclinaba considerablemente hacia la ACP, se convirtió en un mecanismo de dos pilares más equilibrado: se preserva la función principal de la ACP con respecto al tratamiento transfronterizo, pero ahora va acompañada de una función reforzada para las demás autoridades de control que participan activamente en el proceso a través de los mecanismos de cooperación y coherencia, y una función de árbitro y guía para el Comité en caso de desacuerdo.

88. Por tanto, una interpretación teleológica e histórica del RGPD confirma la importancia del mecanismo de ventanilla única y, como consecuencia, la competencia general de la ACP con respecto al

tratamiento de datos transfronterizos. La interpretación de las disposiciones del RGPD planteada por la APD y ciertos gobiernos no puede conciliarse con la intención del legislador de la Unión, como se desprende de la exposición de motivos y de las disposiciones del Reglamento, así como de los trabajos preparatorios.

89. Por lo tanto, concluyo que un enfoque textual, contextual, teleológico e histórico de la interpretación de las disposiciones pertinentes del RGPD confirma que las autoridades de control están obligadas a seguir las reglas sobre competencia, así como las relativas a los mecanismos y procedimientos de cooperación y coherencia establecidos en el Reglamento. Cuando conozcan de un tratamiento transfronterizo, dichas autoridades deben actuar dentro del marco establecido por el RGPD.

90. No obstante, la APD y algunos gobiernos plantearon dos conjuntos adicionales de argumentos que, a su juicio, abogan a favor del fortalecimiento de los poderes de todas las autoridades de control para actuar unilateralmente, incluso con respecto al tratamiento transfronterizo. En las siguientes secciones, explicaré por qué esos argumentos no deben cuestionar la interpretación del RGPD que acabo de sugerir, desde luego no en este momento.

3. Una interpretación del RGPD orientada a la Carta

91. La APD mantiene el criterio de que el poder sin restricciones de las autoridades de control para entablar procedimientos contra los encargados y los responsables del tratamiento, incluso cuando el tratamiento tenga carácter transfronterizo, resulta necesario para garantizar el cumplimiento de los artículos 7, 8 y 47 de la Carta. Parece haber dos preocupaciones principales que sustentan los argumentos de la APD sobre esta materia, aunque no ha articulado plenamente ninguna de ellas en sus observaciones. (41)

92. La *primera* preocupación de la APD parece estar relacionada con la disminución del número de autoridades que pueden actuar sobre una determinada conducta. Parece haber una suposición silenciosa en esa tesis, a saber, que un alto nivel de protección requiere una multiplicidad de autoridades que puedan velar por el cumplimiento del RGPD, incluso actuando en paralelo. En resumidas cuentas, cuantas más autoridades persigan las infracciones, mayor nivel de protección habrá.

93. No creo que esto tenga que ser necesariamente así, al menos en lo que respecta al nivel de protección.

94. Es cierto que, como ha señalado el Tribunal de Justicia, la legislación de la Unión en materia de protección de datos, examinada a la luz de los artículos 7 y 8 de la Carta, se propone garantizar un *elevado nivel* de protección de, entre otros, el derecho fundamental al respeto de la vida privada con respecto al tratamiento de los datos personales. (42)

95. No obstante, el legislador de la Unión ha adoptado el criterio según el cual, para garantizar un «*elevado* nivel de protección de las personas físicas», se requiere un «marco *más* sólido y *coherente* para la protección de datos». (43) Con ese fin, el marco establecido por el RGPD está destinado a garantizar la coherencia en todos los niveles: para las personas físicas, para los operadores económicos, para los responsables y encargados del tratamiento, y para las autoridades de control por igual. (44) Con respecto a estas últimas, el RGPD pretende, como se confirma en el considerando 116, fomentar «una cooperación *más estrecha*» entre ellas. (45)

96. En consecuencia, a diferencia de lo que argumentó la APD, la búsqueda de un *elevado* nivel de protección de los derechos y libertades de los interesados está —a los ojos del legislador de la Unión— plenamente en consonancia con el funcionamiento del mecanismo de ventanilla única antes ilustrado. Al permitir un enfoque más coherente, eficaz y transparente sobre la materia, los mecanismos de cooperación y coherencia establecidos en el RGPD deberían contribuir a una mayor promoción y salvaguardia de los derechos consagrados, entre otros, en los artículos 7 y 8 de la Carta.

97. Dicho de otra manera, un nivel de protección coherente y uniforme ciertamente no impide que la protección se sitúe en un nivel elevado. Se trata simplemente de dónde situar ese criterio uniforme. Al fin y al cabo, resulta dudoso que la coexistencia de varias acciones no relacionadas, y potencialmente contradictorias, por parte de las autoridades de control realmente promueva el objetivo de garantizar un *elevado* nivel de protección de los derechos de las personas. Podría decirse que la coherencia y la claridad, garantizadas por las autoridades de control actuando de forma concertada, sirven mejor a ese objetivo.

98. La *segunda* preocupación expresada por la APD plantea cuestiones de proximidad entre los particulares que presentan una reclamación y las autoridades que, en última instancia, tomarán medidas en respuesta a esa reclamación. La cuestión es, en esencia, si los particulares pueden efectivamente entablar un procedimiento contra la acción o inacción de las autoridades de control frente a sus reclamaciones.

99. De hecho, el artículo 78 del RGPD confirma el derecho de las personas físicas o jurídicas a la tutela judicial efectiva contra una autoridad de control. Además, para ser coherentes con el artículo 47 de la Carta, los recursos previstos en el RGPD no pueden exigir a los interesados que cumplan normas detalladas que, teniendo en cuenta su condición de personas físicas, puedan afectar de forma desproporcionada a su derecho a la tutela judicial (por ejemplo, aumentando los costes o retrasando la acción). (46)

100. No obstante, ninguno de los argumentos (bastante imprecisos) planteados por cada parte sobre este punto explica claramente por qué la interpretación del RGPD planteada por Facebook, los gobiernos checo y finlandés y la Comisión chocaría con el artículo 47 de la Carta.

101. Para empezar, el RGPD establece expresamente el derecho de los interesados a entablar procedimientos tanto contra los responsables y los encargados del tratamiento como contra las autoridades de control. Por lo tanto, en términos estructurales, no es evidente por qué el RGPD no cumpliría el artículo 47 de la Carta.

102. En lo que respecta al derecho de los interesados a entablar acciones *contra los responsables y los encargados del tratamiento*, se les da la opción de iniciar un procedimiento ante los tribunales de los Estados miembros donde el responsable o el encargado del tratamiento tenga un establecimiento o donde residan los interesados. (47) Esta regla parece bastante favorable, o al menos no problemática, para los interesados. (48)

103. En lo que respecta al derecho de los interesados a iniciar acciones c*ontra las autoridades de control*, la situación es más compleja. Para empezar, los interesados tienen derecho a impugnar tanto las actuaciones como la inacción de las autoridades de control. En particular, pueden actuar contra cualquier autoridad de control que «no responda a una reclamación, rechace o desestime total o parcialmente una reclamación o no actúe cuando sea necesario para proteger los derechos del interesado». (49)

104. No obstante, las acciones contra las autoridades de control deben, a diferencia de lo que ocurre con las acciones contra los responsables y los encargados del tratamiento, ejercitarse ante los tribunales del Estado miembro en el que esté establecida la autoridad de control. (50) Si bien esta regla puede parecer menos favorable para los particulares, debe tenerse en cuenta que, a tenor del artículo 60, apartados 8 y 9, del RGPD, cuando se desestime o rechace total o parcialmente una reclamación, la decisión pertinente es adoptada y notificada al interesado *por la autoridad de control ante la que se haya presentado la reclamación*. Esto es así con independencia de que esa autoridad sea o no la ACP, lo que permite (si procede) al interesado ejercitar una acción en su propio Estado miembro.

105. Estos mecanismos de traslado de la competencia para adoptar las decisiones y, cuando sea necesario, de adopción potencial de decisiones en dos niveles (la ACP frente al responsable o encargado del tratamiento, y la autoridad local frente al reclamante) parecen destinados específicamente a evitar que los interesados tengan que «peregrinar» por las salas de audiencias de la Unión para ejercitar acciones contra las autoridades de control inactivas.

106. No obstante, reconozco que esa solución puede plantear una serie de preguntas prácticas. ¿Cuál será el contenido exacto de cada una de esas decisiones? ¿Ese contenido sería idéntico (51) o diferente? ¿Se permitiría que un interesado impugnara todos los aspectos que crea que afectan a su asunto, incluso aquellos que formen efectivamente parte de la decisión de la ACP? ¿O sería la decisión de la autoridad de control ante la cual el interesado presente una reclamación en gran medida un cascarón vacío, que se limite a analizar la reclamación individual de una manera formal, quedando todo el contenido real en la decisión de la ACP? En ese caso, ¿tendría el interesado, para tener acceso a la «tutela judicial efectiva» en el sentido del artículo 78 del RGPD y del artículo 47 de la Carta, que ejercitar acciones en los tribunales del Estado miembro donde esté establecida la ACP en todo caso? ¿Cómo operarían las reglas para el acceso a la tutela judicial efectiva con respecto a la revisión de cualquier decisión subyacente, ya sea en el nivel *horizontal* (entre las autoridades de control que actúan conjuntamente) o en el nivel *vertical* (en lo que respecta a la revisión de un dictamen o una decisión del Comité en el mecanismo de coherencia que preceda y determine efectivamente la decisión definitiva de una autoridad de control)? (52)

107. Los potenciales problemas espinosos no son precisamente pocos. La experiencia práctica podría, algún día, revelar verdaderos problemas con la calidad o incluso el nivel de protección legal inherente al nuevo sistema. No obstante, en la actualidad, cualquiera de estas cuestiones permanece en el terreno de la conjetura. En esta etapa, y ciertamente en este proceso, no se ha presentado al Tribunal de Justicia ningún elemento que apunte a problema real alguno en este sentido.

4. Una posible aplicación insuficiente del RGPD

108. La APD argumenta, en esencia, que la ejecución del RGPD en situaciones transfronterizas no puede dejarse casi exclusivamente en manos de la ACP y de los interesados que pueden verse afectados por el tratamiento. Es precisamente la función de todas y cada una de las autoridades de control actuar a fin de proteger los derechos de las personas que pueden verse afectadas por el tratamiento de datos. En particular, una autoridad de control no puede cumplir adecuadamente con su misión si, en cada ocasión, la decisión de tomar o no medidas contra una presunta infracción, y la manera de hacerlo, queda a la discreción de otra autoridad.

109. A mi juicio, este argumento representa esencialmente una impugnación directa del nuevo mecanismo de cooperación introducido por el RGPD. Mi contestación en respuesta al mismo se formula en dos niveles: por un lado, en lo que respecta al ámbito del *Derecho vigente*, se podría decir que el RGPD contiene mecanismos destinados a evitar tales escenarios. Por otro lado, en lo que respecta al *funcionamiento real y los efectos* de los nuevos sistemas, dichos temores resultan, en esta etapa, prematuros e hipotéticos.

110. En primer lugar, debe aclararse desde el principio que el hecho de que una autoridad de control no sea la ACP con respecto a un determinado responsable o encargado del tratamiento no supone de ninguna manera —como afirma la APD— que las infracciones del RGPD que sean constitutivas de delito no puedan enjuiciarse adecuadamente. El poder de «poner en conocimiento de las autoridades judiciales las infracciones del presente Reglamento», establecido en el artículo 58, apartado 5, incluye obviamente el poder de interactuar con las autoridades penales, como la fiscalía. Ese poder es coherente con la función de las autoridades de control de vigilar y ejecutar la aplicación del RGPD en su territorio y no menoscaba el funcionamiento eficaz de los mecanismos de cooperación y coherencia establecidos en el capítulo VII del RGPD. A este respecto, huelga decir que, si bien estos mecanismos son obligatorios para las autoridades de control, *no se aplican* a *otras* autoridades de los Estados miembros, en particular a las que tienen encomendada la función de perseguir delitos.

111. En segundo lugar, y lo que es más importante, cuando el sistema establecido por el RGPD se contempla en su totalidad, queda bastante claro que la ACP no es el único organismo que vela por el cumplimiento del RGPD en situaciones transfronterizas. La ACP es más bien un *primus inter pares*. Por lo general, una ACP solo podrá actuar (administrativa o judicialmente) con el consentimiento de las ACI. En el marco del procedimiento establecido en el artículo 60 del RGPD, la ACP está obligada a llegar a un consenso. (53) No puede pasar por alto los criterios de las ACI. La ACP no solo está obligada a «tener

debidamente en cuenta» esos criterios, sino que cualquier objeción formal expresada por una ACI tiene el efecto de bloquear temporalmente la adopción del proyecto de decisión de la ACP. En última instancia, toda divergencia persistente de criterios entre las autoridades es resuelta por un organismo específico (el Comité) que está compuesto por representantes de todas las autoridades de control de la Unión. Por lo tanto, la postura de la ACP en ese sentido no es más sólida que la de cualquier otra autoridad. (54)

112. Como señaló el Sr. P. Hustinx, antiguo Supervisor Europeo de Protección de Datos, dentro del esquema del RGPD, el rol de una ACP «no debe verse como una competencia *exclusiva*, sino como una forma estructurada de cooperación con otras autoridades de control localmente competentes». (55) El RGPD establece una responsabilidad compartida para supervisar la aplicación del RGPD y garantizar su aplicación coherente. A tal efecto, se asignan funciones a las autoridades de control y se les dota de determinados poderes; se les conceden algunos derechos, pero también se les imponen algunos deberes. Entre esos deberes se encuentra, en particular, la obligación de seguir ciertos procedimientos y mecanismos destinados a garantizar la coherencia. El deseo de una autoridad de adoptar un enfoque «en solitario» (56) con respecto a la aplicación (judicial) del RGPD, sin cooperar con las demás autoridades, no se puede conciliar ni con la letra ni con el espíritu de ese Reglamento.

113. Como se menciona en los puntos 76 y 77 anteriores, el RGPD se basa en un delicado equilibrio entre la necesidad de garantizar un elevado nivel de protección de las personas físicas y la necesidad de eliminar los obstáculos a la circulación de los datos personales dentro de la Unión. Estos dos objetivos, como lo demuestran en particular el considerando 10 y el artículo 1, apartado 1, del RGPD, están indisolublemente vinculados. Por tanto, las autoridades de control nacionales deben garantizar un equilibrio justo entre ellas, como ha subrayado constantemente el Tribunal de Justicia desde sus primeras sentencias en el ámbito de la protección de datos. (57) El artículo 51, apartado 1, del RGPD, al definir la misión de las autoridades de control, refleja ese enfoque. (58)

114. En tercer lugar, el RGPD no solo proporciona mecanismos para resolver las divergencias con respecto a la manera en que se llevará a cabo la ejecución, es decir, arbitrando entre criterios opuestos y opiniones expresadas por las autoridades de control. Asimismo, incluye mecanismos para superar situaciones de inercia administrativa. Esas son, en particular, las situaciones en las que una ACP —por falta de experiencia y/o personal, o por cualquier otra razón-no adopta ninguna medida significativa para investigar posibles infracciones del RGPD y, cuando corresponda, hacer cumplir sus reglas.

115. Como cuestión de principio, el RGPD requiere, en los casos relacionados con el tratamiento transfronterizo, que la ACP actúe con prontitud. En particular, con arreglo al artículo 60, apartado 3, del RGPD, una ACP «comunicará *sin dilación* a las demás autoridades de control interesadas la información pertinente a este respecto [y] transmitirá *sin dilación* un proyecto de decisión a las demás autoridades de control interesadas para obtener su dictamen al respecto y tendrá debidamente en cuenta sus puntos de vista». (59)

116. En caso de que una ACP incumpla dicha obligación o, de modo más general, no actúe cuando se requiera, cabe preguntarse: ¿existe algún recurso legal para las ACI que estén dispuestas a proceder con una investigación y, posiblemente, a emprender acciones por incumplimiento? (60) Creo que esas autoridades pueden seguir al menos dos vías diferentes, y esas vías se excluyen entre sí.

117. Por un lado, según el artículo 61, apartados 1 y 2, del RGPD, una autoridad de control puede solicitar a otra autoridad de control que facilite «información útil *y* [preste] asistencia mutua a fin de aplicar [el RGPD]». (61) Dicha solicitud puede revestir la forma de una solicitud de información, incluso «sobre el desarrollo de una investigación», o de otras medidas de asistencia (como la realización de inspecciones e investigaciones, o la puesta en marcha de medidas para una cooperación eficaz). Toda solicitud de este tipo debe ser respondida por la autoridad requerida «sin dilación indebida y a más tardar en el plazo de un mes a partir de la solicitud».

118. A tenor del artículo 61, apartados 5 y 8, del RGPD, la falta de respuesta dentro del plazo establecido, o la negativa a atender la solicitud, habilita a la autoridad solicitante a «adoptar una medida provisional en

el territorio de su Estado miembro de conformidad con lo dispuesto en el artículo 55, apartado 1». En tales casos, «se *supondrá* que existe la necesidad urgente contemplada en el artículo 66, apartado 1, que exige una decisión urgente y vinculante del Comité en virtud del artículo 66, apartado 2». (62)

119. Me parece que ese mecanismo también puede utilizarse (y probablemente esté destinado a ser utilizado (63)) por una ACI frente a una ACP. La falta de actuación en un caso específico de tratamiento transfronterizo por parte de la ACP, a pesar de una solicitud a tal efecto por parte de una ACI, puede, por tanto, permitir a esta última adoptar las medidas urgentes que se consideren necesarias para proteger los intereses de los interesados. De hecho, se presume la existencia de circunstancias excepcionales que justifican la necesidad urgente de actuar, de modo que no es necesario probarla.

120. Por otro lado, el artículo 64, apartado 2, del RGPD permite a cualquier autoridad de control (o el presidente del Comité o la Comisión) «solicitar que cualquier asunto de aplicación general o *que surta efecto en más de un Estado miembro* sea examinado por el Comité a efectos de dictamen, *en particular cuando una autoridad de control competente incumpla las obligaciones relativas a la asistencia mutua con arreglo al artículo 61* […]». (64)

121. No está del todo claro si la decisión del Comité sería *legalmente* vinculante para la ACP de que se trate. (65) No obstante, con arreglo al artículo 65, apartado 1, letra c), del RGPD, cuando una autoridad de control competente no siga el dictamen del Comité emitido en virtud del artículo 64, cualquier ACI (o la Comisión) podrá ponerlo en conocimiento del Comité e iniciar así el procedimiento de resolución de conflictos a tal fin. Este último procedimiento, a la postre, daría lugar a una decisión vinculante. (66)

122. Dicho esto, hay que reconocer que los dos mecanismos ilustrados anteriormente (los artículos 61 y 66 del RGPD, por un lado, y los artículos 64 y 65 del RGPD por otro lado), son algo engorrosos. Su funcionamiento real no siempre resulta claro. Por tanto, si bien sobre el papel las disposiciones mencionadas parecen aptas para evitar esos problemas, solo su aplicación futura dirá si, en la práctica, pueden acabar siendo «tigres de papel».

123. Esto me lleva de nuevo al segundo eje del argumento planteado en relación con la aplicación insuficiente, y su naturaleza bastante hipotética e injustificada, particularmente en el momento actual. Debo admitir que, al menos para mí, si se materializaran los peligros relacionados con la aplicación insuficiente del RGPD que sugiere la APD y algunas otras partes coadyuvantes, habría llegado el momento de revisar profundamente todo el sistema.

124. Desde un punto de vista estructural, esto podría suceder si la nueva estructura diera lugar a «refugios» normativos para ciertos operadores que, tras haber elegido ellos mismos efectivamente su regulador nacional situando en consecuencia su establecimiento principal dentro de la Unión, en lugar de ser controlados, quedarían de hecho protegidos por una ACP determinada frente a los demás reguladores. Casi nadie dudaría de que la competencia normativa en forma de carrera a la baja entre los Estados miembros sería tan malsana y peligrosa como la incoherencia normativa, que es el tipo de falta de coordinación y coherencia característico del sistema anterior. Una red de regímenes regulatorios podría prevenir la incoherencia y la divergencia fomentando el consenso y la cooperación. No obstante, el precio del consenso tiende a ser el bloqueo de las autoridades activas, especialmente en un sistema donde se precisa una mayor concertación para alcanzar cualquier decisión. En tal sistema, la responsabilidad colectiva puede inducir a la irresponsabilidad colectiva y, en última instancia, a la inercia.

125. No obstante, con respecto a tales peligros, el marco jurídico establecido por el RGPD aún está en pañales. No es fácil predecir —especialmente para un tribunal, en el contexto de un procedimiento único, o más bien singular— cómo funcionarán en la práctica los mecanismos establecidos por ese Reglamento y cuán eficaces serán. Dentro de ese marco, al igual que sucede con los posibles problemas bajo el epígrafe de la protección de los derechos fundamentales y la interpretación conforme a la Carta, (67) se aconseja precaución.

126. A mi juicio, sería una mala idea que el Tribunal de Justicia alterase significativamente ese marco —que es el producto (delicado y cuidadosamente elaborado) de un proceso legislativo largo e intenso— mediante la interpretación de frases aisladas sacadas de su contexto y, en este momento, sobre la base de presunciones y especulaciones. Esto es aún más cierto si la interpretación propuesta por algunas partes es simplemente la de excluir en esencia del Reglamento algunas partes clave y así volver *de facto* al antiguo sistema de la Directiva 95/46, que, en su dimensión institucional, ha sido descartado expresa y claramente por el legislador de la Unión.

127. Ese diseño legislativo meridianamente claro, evidenciado, como se desprende de las secciones anteriores de las presentes conclusiones, tanto en el texto como en la estructura del RGPD, así como en la intención legislativa documentada, proporciona igualmente una respuesta a otras potenciales preocupaciones estructurales, tales como las relacionadas con el equilibrio adecuado entre la aplicación pública y privada de las normas de protección de datos y el RGPD. ¿Tiene sentido limitar la ejecución *pública* a una sola autoridad y, por lo tanto, a un solo Estado miembro, que solo se producirá después de un procedimiento administrativo largo y engorroso, considerando que es probable que la ejecución *privada* de las mismas reglas se produzca más rápidamente en la práctica y ante los tribunales (civiles) de todos los Estados miembros? ¿Deberían las autoridades de control nacionales tener un acceso a los tribunales más limitado que cualquier consumidor privado individual? ¿No acabará la mayoría de los asuntos de protección de datos en los tribunales nacionales (y posiblemente ante el Tribunal de Justicia por vía de decisión prejudicial), entablados directamente por litigantes privados, pasando por alto por completo a los reguladores nacionales establecidos para tal fin, porque aún se encuentren en el proceso de cooperar y coordinar sus posiciones? Dentro de tal régimen, ¿no existe el peligro de que la ejecución privada sustituya por completo a la pública?

128. Sea como fuere, el legislador de la Unión hizo una elección institucional y estructural clara y, a mi juicio, no hay duda sobre lo que pretendía lograr. En tales circunstancias, dicho metafóricamente, debería darse a la criatura el beneficio de la duda, al menos por el momento. No obstante, si el niño se tuerce, y se acreditase mediante hechos y argumentos sólidos, entonces no creo que el Tribunal de Justicia hiciera la vista gorda ante cualquier laguna que pudiera surgir en la protección de los derechos fundamentales garantizados por la Carta y su aplicación efectiva por parte de los reguladores competentes. En cuanto a si la cuestión se refiere a una interpretación de las disposiciones del derecho secundario conforme a la Carta, o a un problema de validez de las disposiciones pertinentes, o incluso de los apartados de un instrumento de derecho secundario, ese es un extremo que debería resolverse en otro asunto.

5. Conclusión provisional

129. Por tanto, todos los elementos interpretativos descritos apuntan a un mismo resultado: la ACP tiene una competencia general sobre el tratamiento transfronterizo. Todas las autoridades de control (independientemente de su función como ACP o ACI) deben actuar, especialmente en el caso del tratamiento transfronterizo, con arreglo a los procedimientos y mecanismos establecidos en el RGPD.

130. Dicho esto, ¿se deduce de ello que una autoridad de control que no sea la ACP tiene siempre vedado, como cuestión de principio, actuar ante los tribunales nacionales contra un responsable o encargado del tratamiento cuando el tratamiento tenga carácter transfronterizo?

131. La respuesta es no.

132. En primer lugar, las autoridades de control pueden, como es natural, acudir a un tribunal nacional cuando actúen fuera del ámbito material del RGPD, siempre que ello esté permitido por la legislación nacional y no esté vedado por la legislación de la Unión, por ejemplo, porque el tratamiento no afecte a datos personales o porque el tratamiento de datos personales se lleve a cabo en el contexto de las actividades mencionadas en el artículo 2, apartado 2, del RGPD. (68)

133. En segundo lugar, a pesar del carácter transfronterizo del tratamiento, en las situaciones previstas en el artículo 55, apartado 2, del RGPD (tratamiento realizado por autoridades públicas, pero también

cualquier tratamiento realizado en interés público o en el ejercicio de poderes públicos), la competencia reguladora permanece en manos de la autoridad de control local, lo cual naturalmente también incluye, si surge la necesidad, la legitimación activa ante los tribunales.

134. En tercer lugar, hay casos en los que, a pesar de que existe un tratamiento transfronterizo de datos personales que recae dentro del ámbito del RGPD, ninguna autoridad de control puede actuar como ACP. Dado que el mecanismo de cooperación y coherencia establecido en el RGPD solo se aplica a los responsables del tratamiento con uno o más establecimientos en la Unión, no hay ninguna ACP con respecto al tratamiento transfronterizo realizado por los responsables del tratamiento que no tengan un establecimiento en la Unión. Esto significa que los responsables del tratamiento sin ningún establecimiento en la Unión deben tratar con las autoridades de control locales en todos los Estados miembros en los que operan. (69)

135. En cuarto lugar, cualquier autoridad de control puede adoptar medidas urgentes cuando se cumplan las condiciones adecuadas. Además, existen situaciones en las que se presume la urgencia de las medidas. Eso puede suceder, por ejemplo, en los casos en que una ACI se enfrente potencialmente a la inercia persistente de la ACP encargada. Dado que el artículo 66, apartado 1, del RGPD prevé un apartamiento integral del mecanismo de coherencia, es justo suponer que, en una situación tan excepcional, toda la gama de poderes conferidos a una autoridad de control (que en circunstancias normales no debe ser ejercida porque se ve bloqueada por las normas especiales sobre la competencia de una ACP para el tratamiento transfronterizo) se reactiva y puede ejercerse temporalmente. Esto, por lo tanto, incluye naturalmente la facultad de iniciar acciones judiciales a tenor de lo dispuesto en el artículo 58, apartado 5, del RGPD.

136. En quinto y último lugar, en aras de la exhaustividad, cabe señalar que existe igualmente la posibilidad de que una autoridad de control que informe a la ACP también pueda adquirir (o más bien conservar) el poder de acudir a los tribunales en un caso en el que la ACP «decida no tratar el caso» con arreglo al artículo 56, apartado 5, del RGPD. A primera vista, esta última disposición podría dar buena cabida a un acuerdo efectivo entre ambas autoridades de control sobre cuál de ellas está en mejores condiciones para tratar un caso.

137. En resumen, las disposiciones del RGPD no incluyen ningún *impedimento general* a que otras autoridades de control, especialmente las ACI, inicien procedimientos contra posibles infracciones de las normas de protección de datos. Por el contrario, las diversas situaciones en las que están facultadas para ello están expresamente previstas en el RGPD, o se derivan implícitamente de este. (70)

138. En general, sin embargo, es de suma importancia que, cuando se apliquen los procedimientos y mecanismos previstos en el RGPD (especialmente los recogidos en los capítulos VI y VII de este), tanto la ACP como las ACI se atengan a ellos debidamente. Las reglas del RGPD son muy claras en el sentido de que ninguna de esas autoridades debe actuar fuera de ese marco jurídico o pasándolo por alto.

139. Dicho esto, la cuestión de si la APD ha cumplido o no con esos procedimientos y mecanismos en el caso que nos ocupa —un tema que dio lugar a cierto debate en la vista, pero que sigue siendo un tanto confuso habida cuenta del peculiar trasfondo procesal del presente caso (71)— es algo que corresponde comprobar, no obstante, al tribunal remitente.

140. Por consiguiente, la respuesta a la primera cuestión prejudicial debería ser que las disposiciones del RGPD *permiten* que la autoridad de control de un Estado miembro ejercite acciones judiciales ante un tribunal de ese Estado por una presunta infracción del RGPD con respecto al tratamiento transfronterizo de datos, aunque no sea la ACP, *siempre que* lo haga en las situaciones y con arreglo a los procedimientos establecidos en el RGPD.

C. Sobre las demás cuestiones prejudiciales planteadas

1. Segunda cuestión prejudicial

141. Mediante su segunda cuestión prejudicial, el tribunal remitente pregunta si la respuesta a la primera cuestión sería diferente si el responsable del tratamiento transfronterizo no tuviera su establecimiento principal en ese Estado miembro, pero sí otro establecimiento en este.

142. Habida cuenta de la respuesta propuesta para la primera cuestión prejudicial, la respuesta a la segunda cuestión prejudicial es bastante clara: en principio, *no*, siempre que el «establecimiento principal» en el sentido del artículo 4, apartado 16, del RGPD se encuentre efectivamente en otro Estado miembro.

143. El hecho de que un responsable del tratamiento tenga un establecimiento *secundario* en un Estado miembro, en principio, no afecta a la capacidad de la autoridad de control local para entablar un procedimiento judicial, de conformidad con el artículo 58, apartado 5, del RGPD, en relación con un determinado tratamiento transfronterizo. Es decir, en el caso del tratamiento transfronterizo de datos, el alcance de los poderes otorgados a una autoridad de control y la forma en que dichos poderes deben ejercerse no dependen generalmente de que el responsable o el encargado del tratamiento, que tenga su establecimiento principal en otro Estado miembro, tenga *también* un establecimiento en el Estado miembro de dicha autoridad.

144. No obstante, de manera similar a lo que ya se ha señalado anteriormente, (72) como elemento preliminar a esta conclusión, el tribunal nacional debe determinar en primer lugar qué establecimiento es efectivamente el establecimiento principal *a efectos de una determinada operación de tratamiento*. En ese sentido, el artículo 4, apartado 16, letra a), del RGPD adopta una concepción dinámica (73) de lo que se considera el establecimiento principal, que no tiene por qué coincidir necesariamente con la estructura societaria estática de una empresa.

145. Además, el hecho de que el responsable o el encargado del tratamiento tenga un establecimiento (secundario) en el territorio de la autoridad de control significa que dicha autoridad es una ACI en el sentido del artículo 4, apartado 22, del RGPD. A los ACI se les otorgan poderes significativos en el ámbito de los procedimientos establecidos en el capítulo VII del RGPD. (74)

146. Además, el artículo 56, apartado 2, del RGPD establece una excepción a la competencia general de la ACP con respecto al tratamiento transfronterizo: «cada autoridad de control será competente para tratar una reclamación que le sea presentada o una posible infracción del [RGPD], en caso de que se refiera únicamente a un establecimiento situado en su Estado miembro o únicamente afecte de manera sustancial a interesados en su Estado miembro». Esta competencia debe, a su vez, ejercerse de conformidad con el procedimiento previsto en los apartados 3 a 5 de la misma disposición. (75)

2. Tercera cuestión prejudicial

147. Mediante su tercera cuestión prejudicial, el tribunal remitente pregunta si la respuesta a la primera cuestión prejudicial sería diferente si la autoridad de control nacional incoara un procedimiento judicial contra el establecimiento principal del responsable del tratamiento o contra el establecimiento situado en su propio Estado miembro.

148. Habida cuenta de la respuesta propuesta a la primera cuestión prejudicial, y en la medida en que la tercera cuestión no se solapa de hecho con la segunda cuestión, la tercera pregunta también amerita una respuesta negativa.

149. Una vez más, siempre que se haya aclarado efectivamente en función de los hechos de un asunto que el establecimiento principal para una operación de tratamiento determinada con arreglo al artículo 4, apartado 16, del RGPD está realmente situado en otro Estado miembro, la autoridad de control nacional del Estado miembro en el que se encuentre un establecimiento del responsable del tratamiento no es la ACP, pero podría convertirse en una ACI. Pero dentro de esa apreciación, la competencia de la autoridad de control para actuar no depende de que el procedimiento judicial se entable contra el establecimiento principal del responsable del tratamiento o contra el establecimiento situado en su propio Estado miembro. (76)

150. En aras de la exhaustividad, cabe añadir que el artículo 58, apartado 5, del RGPD está formulado de manera amplia y no especifica las entidades contra las cuales las autoridades de control deberían o podrían actuar. Eso condujo a una interesante exposición en las observaciones de algunas de las partes sobre un tema que no carece de importancia, pero que, a mi juicio, el Tribunal de Justicia no ha de abordar en el presente asunto. El tema es el siguiente: ¿pueden las autoridades de control, siempre que sean efectivamente competentes para hacerlo conforme a las normas del RGPD, actuar únicamente contra el establecimiento o los establecimientos del responsable o del encargado del tratamiento ubicado(s) en su territorio, o también pueden actuar *contra los establecimientos situados en el extranjero*?

151. Por un lado, los Gobiernos belga, italiano y polaco subrayan que el artículo 55, apartado 1, del RGPD limita la competencia territorial de cada autoridad de control a su territorio. De ello deducen que las autoridades de control solo pueden actuar contra los establecimientos establecidos en dicho territorio.

152. No obstante, a mi juicio, el texto no es tan claro: habla de ejercer los poderes conferidos por el Reglamento «en el territorio de su Estado miembro». No considero que esta disposición impida necesariamente una acción contra un establecimiento situado en otro Estado miembro. El elemento de territorialidad incluido en el artículo 55, apartado 1, del RGPD, examinado habida cuenta del ámbito general del RGPD en su artículo 1, apartado 1, y su artículo 3, que activa la competencia de una autoridad de control en un caso determinado, se refiere a *los efectos del tratamiento de datos* en el territorio de un Estado miembro. Ese elemento no opera como un límite a las acciones contra los responsables o encargados del tratamiento radicados fuera de las fronteras nacionales.

153. Por otro lado, la APD sugiere que cada autoridad tiene el poder de actuar contra todas las infracciones del RGPD que tengan lugar en su territorio, independientemente de que el responsable o el encargado del tratamiento tenga un establecimiento en su territorio. Eso significa que una autoridad también debería poder incoar procedimientos contra establecimientos situados en el extranjero. A este respecto, la APD se remite a la sentencia del Tribunal de Justicia en el asunto Wirtschaftsakademie Schleswig-Holstein. (77) En dicha resolución, el Tribunal de Justicia declaró que los artículos 4 y 28 de la Directiva 95/46 permitían a la autoridad de control de un Estado miembro ejercer la facultad de entablar acciones judiciales con respecto a un establecimiento de dicha empresa situado en el territorio de ese Estado miembro. Eso sucedía aun cuando dicho establecimiento fuera responsable únicamente de la venta de espacios publicitarios y otras actividades de marketing en el territorio de ese Estado miembro, mientras que la responsabilidad exclusiva de recopilar y tratar datos personales correspondía, para todo el territorio de la Unión, a un establecimiento situado en otro Estado miembro.

154. La APD tiene razón al argumentar que, en la medida en que el RGPD incluye, en esta materia, disposiciones similares a las de la Directiva 95/46, (78) los principios establecidos por el Tribunal de Justicia en Wirtschaftsakademie Schleswig-Holstein también deben ser válidos, *mutatis mutandis*, con respecto al RGPD. No obstante, dicha sentencia solo explicaba cuándo un establecimiento local puede ser demandado por la autoridad, a pesar de que la (parte principal) del tratamiento se llevaba a cabo por un establecimiento situado en otro lugar de la Unión. Esta sentencia, al menos expresamente, no confirmó ni excluyó que la autoridad de control pudiera actuar también contra este último establecimiento.

155. No obstante, me parece que el nuevo mecanismo de ventanilla única, al crear un punto central de ejecución, implica necesariamente que una autoridad de control también puede actuar contra establecimientos ubicados en el extranjero. No estoy seguro de que el nuevo sistema pueda funcionar correctamente si excluye la posibilidad de que las autoridades, y en particular la ACP, actúen contra establecimientos ubicados en otro lugar. (79)

3. Cuarta cuestión prejudicial

156. Mediante su cuarta cuestión perjudicial, el tribunal remitente pregunta si la respuesta a la primera cuestión sería diferente si la autoridad de control nacional ya hubiera iniciado acciones judiciales antes de la fecha de entrada en vigor del RGPD.

157. De entrada, hay que señalar que, en el RGPD, no existen normas transitorias u otras normas que regulen el estado de los procedimientos judiciales pendientes en el momento de la entrada en vigor del nuevo marco.

158. Habida cuenta de eso, a mi juicio, la respuesta a la cuestión debería ser: «depende».

159. Por un lado, en lo que respecta a las infracciones por parte de los responsables o encargados del tratamiento de las normas sobre protección de datos que se cometieron *antes* de la fecha en la que el RGPD comenzó a ser aplicable, creo que esos procedimientos pueden continuar. No veo ninguna buena razón para obligar a las autoridades a poner fin a las acciones de ejecución que se refieran a una *conducta pasada* que era (supuestamente) ilegal cuando se cometió y contra la cual aquellas eran (en aquel momento) competentes para actuar. Una solución diferente conduciría a una especie de amnistía con respecto a determinados incumplimientos de las leyes de protección de datos.

160. Por otro lado, se presenta una situación diferente en lo que respecta a las acciones ejercidas contra incumplimientos que aún no se han materializado, ya que se producen *después* de la fecha en la que el RGPD comenzó a ser aplicable. (80) En ese sentido, como en cualquier otra situación de nuevas normas aplicables a situaciones derivadas del nuevo régimen jurídico, las nuevas normas sustantivas solo serán de aplicación a hechos ocurridos con posterioridad al momento en que el nuevo instrumento comenzara a ser aplicable. (81)

161. Corresponde al tribunal remitente comprobar cuál de los dos escenarios refleja efectivamente el estado actual del litigio principal. (82) Si fuera el primero, sugiero que el procedimiento en curso podría concluirse, ciertamente desde el punto de vista del Derecho de la Unión, siempre que se limite a una posible declaración de infracciones pasadas. Si fuera el segundo, se debería poner fin al procedimiento nacional. En efecto, el nuevo marco estableció un sistema diferente de competencias y poderes, con la consecuencia de que una ACI no puede actuar frente a las infracciones dimanantes del tratamiento transfronterizo fuera de las situaciones específicas ni sin seguir los procedimientos y mecanismos previstos para tal fin.

162. La solución contraria conllevaría una prórroga *de facto* del sistema establecido por la Directiva 95/46, a pesar de que tanto el Derecho de la Unión como el nacional lo han derogado expresamente y sustituido por uno nuevo. Al fin y al cabo, ¿cabe imaginar que si la APD obtuviera realmente un requerimiento judicial que prohibiera a Facebook adoptar en el futuro (y, por cierto, ¿por cuánto tiempo?) las prácticas controvertidas en el procedimiento principal, ello no interferiría con la competencia sobre (la misma) conducta que el RGPD confirió, a partir del 25 de mayo de 2018, a la ACP y a las ACI, y, potencialmente, con decisiones (o resoluciones judiciales) contradictorias emanadas de diferentes Estados miembros?

4. Quinta cuestión prejudicial

163. Mediante su quinta cuestión prejudicial —planteada en caso de que se responda afirmativamente a la primera— el tribunal remitente pretende aclarar si el artículo 58, apartado 5, del RGPD tiene efecto directo, de modo que una autoridad de control nacional pueda invocarlo para iniciar o continuar procedimientos judiciales contra particulares, incluso si dicha disposición no se ha transpuesto específicamente al Derecho nacional.

164. Reitero que el artículo 58, apartado 5, reza así: «Cada Estado miembro dispondrá por ley que su autoridad de control esté facultada para poner en conocimiento de las autoridades judiciales las infracciones del presente Reglamento y, si procede, para iniciar o ejercitar de otro modo acciones judiciales, con el fin de hacer cumplir lo dispuesto en el mismo.»

165. Facebook y los Gobiernos checo y portugués señalan que esa disposición requiere claramente que los Estados miembros hagan algo: establecer disposiciones que permitan a las autoridades ejercitar acciones judiciales. Para ser plenamente operativa, la facultad de ejercitar dichas acciones también puede requerir

algunas normas nacionales para determinar, entre otros extremos, los tribunales que sean competentes, las condiciones para iniciar una acción y los procedimientos que deben seguirse.

166. Habida cuenta de la respuesta que propongo a la primera cuestión prejudicial, no es necesario responder a la quinta. No obstante, en aras de la exhaustividad, por mi parte, no veo ningún problema en estar de acuerdo con la APD en que el contenido prescriptivo de esa disposición particular del Derecho de la Unión es bastante inequívoco y de aplicación directa. A este respecto, debe tenerse en cuenta que, en general, una disposición del Derecho de la Unión tiene efecto directo siempre que, en lo que respecta a su objeto, sea lo suficientemente clara, precisa e incondicional como para ser invocada contra una medida nacional contradictoria, o en la medida en que la disposición defina derechos que los particulares pueden hacer valer contra el Estado. (83)

167. Aparte del hecho de que la disposición figura incluida en un reglamento (instrumento que, en virtud del artículo 288 del TFUE, es «obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro» (84)), me parece que del artículo 58, apartado 5, del RGPD se puede extraer una norma específica e inmediatamente aplicable. Esa regla es muy simple: las autoridades de control deben contar con legitimación ante los tribunales nacionales, se les confiere la capacidad de iniciar acciones judiciales en la legislación nacional. El recurso interpuesto ante un tribunal nacional no puede declararse inadmisible por falta de personalidad jurídica.

168. Si bien estoy de acuerdo con Facebook y los gobiernos checo y portugués en que los Estados miembros pueden establecer reglas, condiciones o competencias específicas respecto de las acciones ejercitadas por las autoridades de control, tales reglas no son de ninguna manera necesarias para que opere la regla del artículo 58, apartado 5, del RGPD, que es directamente aplicable. A falta de normas *ad hoc* introducidas por el legislador nacional, las normas *por defecto* de los códigos procesales nacionales correspondientes (ya sean códigos de procedimiento contencioso-administrativo o incluso de procedimiento civil por defecto) serán naturalmente aplicables a cualquier acción entablada por las autoridades de control. Así, por ejemplo, si no hubiera reglas de desarrollo específicas en materia de competencia, puede presumirse que sería aplicable la norma general por defecto que probablemente se encuentre en cualquier código de procedimiento (civil), según la cual, salvo disposición en contrario, el tribunal competente es el tribunal del lugar de establecimiento del demandado.

5. Sexta cuestión prejudicial

169. Mediante su sexta y última cuestión prejudicial, el tribunal remitente pregunta si, en caso de que la autoridad de control nacional esté facultada para actuar, el resultado de dicho procedimiento impide que la autoridad de control principal llegue a una conclusión en contrario, en el supuesto de que la autoridad de control principal investigue las mismas o similares actividades de tratamiento transfronterizo de conformidad con el mecanismo establecido en los artículos 56 y 60 del RGPD.

170. Habida cuenta de la respuesta propuesta a la primera cuestión, no es preciso responder a esta cuestión.

171. No obstante, el tema planteado por la presente cuestión muestra una vez más por qué la primera cuestión debe responderse de la manera antes propuesta. Si se eliminara la naturaleza obligatoria de los mecanismos de coherencia y cooperación establecidos en el RGPD, convirtiendo así el mecanismo de ventanilla única en «opcional» o, en realidad, más bien en inexistente, la coherencia de todo el sistema se vería gravemente afectada. Las reglas sobre competencia contenidas actualmente en el RGPD serían, en esencia, reemplazadas por una «carrera hasta la primera sentencia» por parte de todas las autoridades de control. A la postre, quien «llegara primero a la meta» de una sentencia firme dentro de su jurisdicción se convertiría en la ACP efectiva para el resto de la Unión, como se deduce implícitamente de la sexta cuestión prejudicial.

V. Conclusiones

172. Propongo que el Tribunal de Justicia responda a las cuestiones prejudiciales planteadas por el hof van beroep te Brussel (Tribunal de Apelación de Bruselas, Bélgica) de la siguiente manera:

«– Las disposiciones 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 (Reglamento general de protección de datos) permiten que la autoridad de control de un Estado miembro ejercite acciones judiciales ante un tribunal de ese Estado por una presunta infracción de dicho Reglamento con respecto al tratamiento transfronterizo de datos, aunque no sea la autoridad de control principal, siempre que lo haga en las situaciones y con arreglo a los procedimientos establecidos en ese mismo Reglamento.

– El Reglamento General de Protección de Datos impide que una autoridad de control continúe con los procedimientos judiciales iniciados antes de la fecha en la que dicho Reglamento comenzó a ser aplicable, pero que se refieran a conductas ocurridas después de esa fecha.

– El artículo 58, apartado 5, del Reglamento General de Protección de Datos tiene efecto directo, en la medida en que una autoridad nacional de control puede invocarlo para iniciar o continuar procedimientos judiciales ante los tribunales nacionales, incluso si esa disposición no se ha transpuesto específicamente al Derecho nacional.»

---

1 Lengua original: inglés.

---

2 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO 2016, L 119, p. 1).

---

3 DO 1995, L 281, p. 31.

---

4 Por las razones expuestas anteriormente, véase el punto 23 de las presentes conclusiones.

---

5 En ese sentido, el Tribunal de Justicia ha afirmado reiteradamente que, con arreglo a la Directiva 95/46, el concepto de «responsable del tratamiento» ha de interpretarse en sentido amplio (véanse, por ejemplo, las recientes sentencias de 29 de julio de 2019, Fashion ID, C-40/17, EU:C:2019:629, apartados 65, 66 y 70, y de 10 de julio de 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, apartado 66). No veo ninguna razón por la que no pueda predicarse lo mismo con respecto al RGPD.

---

6 Véase, por ejemplo, la sentencia de 25 de julio de 2018, Confédération paysanne y otros (C-528/16, EU:C:2018:583), apartados 72 y 73 y jurisprudencia citada, o de 1 de octubre de 2019, Blaise y otros (C-616/17, EU:C:2019:800), apartado 35.

---

7 Por ejemplo, en mis conclusiones presentadas en el asunto Fashion ID, he explicado las razones por las cuales tanto las normas de la Directiva 95/46 entonces vigente como las de la denominada Directiva de Privacidad Electrónica [Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO 2002, L 201,

p. 37)] podrían ser potencialmente aplicables en un asunto que conlleve la inserción de *cookies* (C-40/17, EU:C:2018:1039), puntos 111 a 115. Sobre este tema, de forma más general, véase el dictamen 5/2019 del Comité Europeo de Protección de Datos sobre la interacción entre la Directiva de Privacidad Electrónica y el RGPD, en particular en lo que respecta a la competencia, las funciones y los poderes de las autoridades de protección de datos, de 12 de marzo de 2019. Véase también el Documento 02/2013 del Grupo de Trabajo sobre Protección de Datos del Artículo 29, que ofrece orientaciones sobre la obtención del consentimiento para las *cookies*, 1676/13/EN WP. 208, de 2 de octubre de 2013.

---

8 El subrayado es mío.

---

9 El subrayado es mío.

---

10 El subrayado es mío.

---

11 En la doctrina jurídica, véase Bensoussan, A.(ed.): *Règlement européen sur la protection des données — Textes, commentaires et orientations pratiques*, 2.ª ed., Bruylant, Bruselas, 2017, p. 363.

---

12 De modo similar, Hijmans, H.: «Comment to Article 56 of the GDPR», en Kuner, C., Bygrave, L., Docksey, C. (eds), *The EU General Data Protection Regulation (GDPR) — A Commentary*, Oxford University Press, Oxford, 2020, p. 921.

---

13 Por analogía con el Derecho administrativo general (o los códigos de procedimiento judicial), un órgano podría tener el *poder* (general) de actuar de determinadas formas, pero no tener necesariamente la *competencia* (*rationae materiae, personae, temporis, loci*...) para utilizar ese poder y para resolver un caso individual. Así, por ejemplo, el hecho de que un tribunal penal tenga la facultad de dictar una sentencia penal no significa necesariamente que también sea competente para hacerlo en el caso de un delito determinado cometido por una persona determinada (un tribunal diferente podría ser competente para ello).

---

14 Comité Europeo de Protección de Datos, dictamen 8/2019 sobre la competencia de una autoridad de control en caso de cambio de circunstancias relativas al establecimiento principal o único, de 9 de julio de 2019, puntos 19 y 20.

---

15 Dicha disposición, en la parte pertinente, rezaba así: «la autoridad de control dispondrá, en particular, de […] capacidad procesal en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la presente Directiva o de poner dichas infracciones en conocimiento de la autoridad judicial».

---

16 Véase Comisión Europea, Primer Informe sobre la aplicación de la Directiva sobre protección de datos (Directiva 95/46) de 15 de mayo de 2003, COM(2003) 265 final, pp. 12 y 13, y su anexo titulado «Análisis y evaluación de impacto sobre la aplicación de la Directiva 95/46 en los Estados miembros», p. 40. Véase también Agencia de los Derechos Fundamentales de la Unión Europea, Access to data protection remedies in EU Member States — Informe, 2012, especialmente pp. 20 a 22.

---

17 Véanse los puntos 51, 57 y 58 de las presentes conclusiones.

18 Sentencias de 6 de octubre de 2015, Schrems (C-362/14, EU:C:2015:650), apartado 63, y de 16 de julio de 2020, Facebook Ireland y Schrems (C-311/18, EU:C:2020:559), apartado 109.

---

19 En algunos casos, una ACI está facultada para (y, por lo tanto, debería poder) presentar a la ACP un proyecto de decisión: véase el artículo 56, apartados 2 a 4, del RGPD.

---

20 Véase, en este sentido, el considerando 125 del RGPD.

---

21 Sentencia de 16 de julio de 2020 (C-311/18, EU:C:2020:559), apartado 120 (el subrayado es mío). Del mismo modo, dejando claro que corresponde a la autoridad de control *competente* reaccionar ante una infracción del RGPD y elegir los medios más adecuados para hacerlo, véanse las conclusiones del Abogado General Saugmandsgaard Øe presentadas en el asunto Facebook Ireland y Schrems (C-311/18, EU:C:2019:1145), puntos 147 y 148. Compárense esas declaraciones con la sentencia de 6 de octubre de 2015, Schrems (C-362/14, EU:C:2015:650), apartado 65, en la que el Tribunal de Justicia afirmó que, con arreglo a la Directiva 95/46, (cualquier) autoridad de control nacional debe tener capacidad para comparecer en juicio.

---

22 Como decía la famosa frase en *El bueno, el feo y el malo* (una película de 1966 dirigida por Sergio Leone, protagonizada por Clint Eastwood, Lee Van Cleef y Eli Wallach, producida por Produzioni Europee Associate y United Artists).

---

23 Artículo 68 del RGPD.

---

24 Véase, en particular, el artículo 70, apartado 1, letra a), del RGPD.

---

25 Véase la exposición de motivos de la propuesta de la Comisión de Reglamento del Parlamento Europeo y del Consejo 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 (Reglamento general de protección de datos), COM(2012) 11 final. Véanse también los considerandos 10, 13 y 123 del RGPD.

---

26 Sobre este tema, véase en general Giurgiu, A. y Larsen, T.: «Roles and Powers of National Data Protection Authorities — Moving from Directive 95/46/EC to the GDPR: Stronger y More “European” APDs as Guardians of Consistency?» *European Data Protection Law Review*, 2016, pp. 342 a 352, en 349; y Voigt, P., von dem Bussche, A.: *The EU General Data Protection Regulation (GDPR) — A Practical Guide*, Springer, 2017, pp. 190 a 192.

---

27 Sentencia de 1 de octubre de 2015 (C-230/14, EU:C:2015:639), apartados 42 a 60.

---

28 Sentencia de 5 de junio de 2018 (C-210/16, EU:C:2018:388), apartados 65 a 74.

---

29 Véase, por ejemplo, Miglio, A.: «The Competence of Supervisory Authorities and the One-stop-shop Mechanism», en EU Law Live — Weekend edition, n.º 28, 2020, pp. 10 a 14, en 11.

30 Véanse las conclusiones del Abogado General Bot presentadas en el asunto Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2017:796), punto 103.

31 Sentencia de 24 de septiembre de 2019 (C-507/17, EU:C:2019:772), apartado 68.

32 C-311/18, EU:C:2019:1145, punto 155.

33 Véanse los considerandos 97 y 98 de la propuesta de la Comisión (véase la nota 25 anterior).

34 Véanse los documentos del Consejo 5419/1/16 REV 1, de 28 de noviembre de 2014, y 16526/14, de 4 y 5 de diciembre de 2014, pp. 2, 8 y 9.

35 *Ibidem*, p. 1.

36 Véase el Documento del Consejo 5419/1/16 REV 1, de 8 de abril de 2016, pp. 203 a 205.

37 Véase el punto 45 de las presentes conclusiones.

38 Documento del Consejo 15656/1/14 REV 1, de 28 de noviembre de 2014, p. 2.

39 Véase el Documento A7-0402/2013, de 22 de noviembre de 2013, que se refirió al mecanismo de ventanilla única como un «paso enorme hacia una aplicación coherente de la legislación en materia de protección de datos en toda la Unión».

40 Documento EP-PE_TC1-COD(2012) 0011, de 12 de marzo de 2014 (véanse especialmente las enmiendas 148, 149, 158, 159 y 167).

41 En la misma óptica, simplemente supongo que las disposiciones de la Carta y los derechos invocados son los de los interesados, que una autoridad de control está llamada a proteger, y no que la titularidad de esos derechos corresponda a la propia autoridad de control. La idea de que las autoridades administrativas, es decir, emanaciones del Estado, estarían dotadas de derechos (humanos) fundamentales que podrían esgrimir contra el Estado (o más bien entre sí o, en casos de efecto directo horizontal, incluso contra los particulares) resulta sin duda bastante peculiar. A mi juicio, la respuesta debería ser claramente negativa, pero reconozco que existen diferentes enfoques dentro de los Estados miembros. Sea como fuere, en el contexto del presente asunto, este problema puede con seguridad dejarse sin explorar.

42 Véase, en ese sentido, la sentencia de 6 de octubre de 2015, Schrems (C-362/14, EU:C:2015:650), apartado 39.

43 Véanse los considerandos 7, 9 y 10 del RGPD (el subrayado es mío).

---

44 Véanse, en ese sentido, los considerandos 10, 11 y 13 del RGPD.

---

45 El subrayado es mío.

---

46 Véase, en ese sentido, la sentencia de 27 de septiembre de 2017, Puškár (C-73/16, EU:C:2017:725), apartados 54 a 76 y jurisprudencia citada.

---

47 Véase el artículo 79 y también el considerando 145 del RGPD.

---

48 Teniendo igualmente en cuenta que, en la práctica, esa solución coincide con lo que normalmente sería el foro (*actoris*) (bastante protector) en los contratos con consumidores bajo el régimen del Reglamento de Bruselas (véase, en general, la sentencia de 25 de enero de 2018, Schrems, C-498/16, EU:C:2018:37).

---

49 Véanse los considerandos 141 y 143 del RGPD, y la sentencia de 16 de julio de 2020, Facebook Ireland y Schrems (C-311/18, EU:C:2020:559), apartado 110.

---

50 Véanse el considerando 143 y el artículo 78 del RGPD.

---

51 En cuanto a este enfoque en otro contexto regulatorio (descentralizado), véanse mis conclusiones presentadas en el asunto Astellas Pharma (C-557/16, EU:C:2017:957).

---

52 Sobre esta última cuestión, el artículo 78, apartado 4, señala que «cuando se ejerciten acciones contra una decisión de una autoridad de control que haya sido precedida de un dictamen o una decisión del Comité en el marco del mecanismo de coherencia, la autoridad de control remitirá al tribunal dicho dictamen o decisión». En términos prácticos, es probable que esta sea la única vía para una revisión judicial de las decisiones del Comité, ya que, como confirma de modo inquietante el considerando 143 del RGPD, «toda persona física o jurídica» (incluidos, por tanto, los interesados) puede, cuando se satisfagan las condiciones establecidas en el artículo 263 del TFUE, impugnar una decisión legalmente vinculante del Comité ante los Tribunales de la Unión. Sin embargo, habida cuenta de la interpretación restrictiva del Tribunal Justicia de las condiciones de legitimación de los particulares establecidas en el artículo 263, apartado 4, del TFUE, no es fácil identificar situaciones en las que se pueda considerar que los particulares se ven *directamente* afectados por las decisiones del Comité, ya que estas últimas decisiones deberán, en cualquier caso, ser «aplicadas» a la situación de un interesado específico mediante una decisión posterior de la ACP o una ACI. En tal situación, como en otros muchos ámbitos del Derecho de la Unión (de manera crítica sobre esta estructura, véanse mis conclusiones presentadas en el asunto Région de Bruxelles-Capitale/Comisión, C-352/19 P, EU:C:2020:588, puntos 137 a 147), la única forma de impugnar una decisión del Comité sería en última instancia mediante una decisión prejudicial con arreglo al artículo 267 del TFUE, limitada a los supuestos en los que un tribunal nacional más inquisitivo desee «levantar el velo» de su propia revisión judicial, colocado frente a él por la autoridad de control nacional en la forma del dictamen «remitido» del Comité con arreglo al artículo 78, apartado 4, del RGPD.

---

53 Véase especialmente el artículo 60, apartado 1, del RGPD.

54 Hijmans, H.: «Comment to Article 56 of the GDPR», en Kuner, C., Bygrave, L., Docksey, C. (eds), *The EU General Data Protection Regulation (GDPR) — A Commentary*, Oxford University Press, Oxford, 2020, p. 918.

55 Hustinx, P.: «EU Data Protection Law: The Review de Directive 95/46/EC and the General Data Protection Regulation», en Cremona, M. (ed.), *New Technologies and EU Law*, 2017, Oxford University Press, Oxford, p. 123.

56 En cuanto a esa expresión, véase Consejo, «Debate político sobre el mecanismo de ventanilla única», 10139/14, de 26 de mayo de 2014, p. 4.

57 Véase, por ejemplo, la sentencia de 9 de marzo de 2010, Comisión/Alemania (C-518/07, EU:C:2010:125), apartado 24. Más recientemente, véase la sentencia de 6 de octubre de 2015, Schrems (C-362/14, EU:C:2015:650), apartado 42.

58 Véase el punto 4 de las presentes conclusiones.

59 El subrayado es mío.

60 En este contexto, me limitaré a añadir que las autoridades de control que reciben una reclamación — independientemente de su condición de ACP o ACI— no solo están obligadas a *examinar* esa reclamación con la debida diligencia (véase el punto 69 de las presentes conclusiones), sino que también están obligadas a «llevar a cabo con toda la diligencia exigible su misión de velar por el pleno *cumplimiento* del RGPD» [véase, a tal efecto, la sentencia de 16 de julio de 2020, Facebook Ireland y Schrems (C-311/18, EU:C:2020:559), apartado 112 (el subrayado es mío)].

61 El subrayado es mío.

62 El subrayado es mío.

63 Véase Tosoni, L.: «Comment to Article 60 of GDPR», en Kuner, C., Bygrave, L., Docksey, C. (eds), *The EU General Data Protection Regulation (GDPR) — A Commentary*, Oxford University Press, Oxford, 2020, p. 969.

64 El subrayado es mío.

65 Dependiendo, según se aclara en el considerando 138 del RGPD, de qué tipo de medida se trate. Sin embargo, en términos realistas, resultaría bastante sorprendente que, incluso si no es formalmente vinculante según el RGPD, una ACP optara por soslayar una decisión del Comité (en particular porque lo que no es vinculante en la primera fase podría serlo, y mucho, en la siguiente).

66 De manera similar, con mayor detalle, Van Eecke, P., Šimkus, A.: «Comment to Article 64», en Kuner, C., Bygrave, L., Docksey, C. (eds), *The EU General Data Protection Regulation (GDPR) — A Commentary*, Oxford University Press, Oxford, 2020, p. 1011.

---

67 Véanse los puntos 106 y 107 de las presentes conclusiones.

---

68 Véanse los puntos 35 a 38 de las presentes conclusiones.

---

69 Véase también Grupo de Trabajo sobre Protección de Datos del Artículo 29, Directrices para determinar la autoridad de control principal de un responsable o encargado del tratamiento, WP. 244 rev.01, de 5 de abril de 2017, p. 10.

---

70 Por otra parte, no pretendo que los ejemplos mencionados sean una lista exhaustiva. Además, ¿no podría haber una situación en la que la decisión final adoptada en un caso determinado de tratamiento transfronterizo — ya sea mediante acuerdo entre la ACP y las ACI, o tras una resolución de conflictos por parte del Comité— pueda encomendar a una o más ACI que lleven a cabo determinados *actos de ejecución* en sus respectivos territorios, incluido, por ejemplo, el ejercicio de acciones judiciales?

---

71 Tal como he expuesto en los puntos 31 a 38 de las presentes conclusiones.

---

72 Véanse los puntos 32 a 33 de las presentes conclusiones.

---

73 Como debe suceder, en general, con respecto a cualquier tratamiento como tal, y la definición de responsable (o corresponsable) del mismo. El control efectivo sobre *los fines y los medios* del tratamiento debe evaluarse con respecto a una *operación de tratamiento determinada*, y no en términos abstractos y estáticos, con respecto a un «tratamiento» indefinido (véase la sentencia de 29 de julio de 2019, Fashion ID, C-40/17, EU:C:2019:629, apartados 71 a 74).

---

74 Véanse los puntos 111 y 112 de las presentes conclusiones.

---

75 Véanse los puntos 45 y 84 de las presentes conclusiones.

---

76 Por lo tanto, volviendo indirectamente al problema inicial de qué es lo que hace exactamente que se entable de hecho un procedimiento contra tal establecimiento en dicho Estado miembro *después* de que el RGPD comenzara a ser aplicable, como se expuso anteriormente en los puntos 32 a 34 de las presentes conclusiones.

---

77 Sentencia de 5 de junio de 2018 (C-210/16, EU:C:2018:388).

---

78 Compárese, en particular, el nuevo artículo 3, apartado 1, con el antiguo artículo 4, apartado 1, letra a), y el nuevo artículo 58, apartado 6, con el antiguo artículo 28, apartado 3, tercer guion.

79 Sin embargo, como se ha sugerido en la nota 70, resulta igualmente concebible que la toma de decisiones coordinada pueda traducirse en medidas de ejecución coordinadas.

---

80 Véase, por analogía, la sentencia de 14 de febrero de 2012, Toshiba Corporation y otros (C-17/10, EU:C:2012:72), especialmente el apartado 60.

---

81 En cuanto a una exposición detallada con ejemplos, véanse mis conclusiones presentadas en el asunto Nemec (C-256/15, EU:C:2016:619), puntos 27 a 44.

---

82 Véase también el punto 34 de las presentes conclusiones.

---

83 Con mayor detalle, véanse mis conclusiones presentadas en el asunto Klohn (C-167/17, EU:C:2018:387), puntos 36 a 46.

---

84 Si bien, por supuesto, la aplicabilidad directa no equivale a efecto directo y las mismas condiciones para el efecto directo se aplican con respecto a las disposiciones de los reglamentos que prevén o requieren su ejecución (véanse, por ejemplo, las sentencias de 11 de enero de 2001, Monte Arcosu, C-403/98, EU:C:2001:6, apartados 26 a 28; de 28 de octubre de 2010, SGS Belgium y otros,C-367/09, EU:C:2010:648, apartados 33 y ss., o de 14 de abril de 2011, Vlaamse Dierenartsenvereniging y Janssens, C-42/10, C-45/10 y C-57/10, EU:C:2011:253, apartados 48 a 50).