Recopilación de la Jurisprudencia

CONCLUSIONES DEL ABOGADO GENERAL
M. CAMPOS SÁNCHEZ-BORDONA
presentadas el 20 de abril de 2023 [1]

Asunto C-548/21

C. G.
contra
Bezirkshauptmannschaft Landeck

[Petición de decisión prejudicial planteada por el Landesverwaltungsgericht Tirol (Tribunal regional de lo contencioso administrativo del Tirol, Austria)]

«Procedimiento prejudicial — Telecomunicaciones — Protección de datos personales — Directiva (UE) 2016/680 — Procedimiento penal — Tentativa de acceso de las autoridades públicas a los datos registrados en un teléfono móvil sin autorización judicial o de una autoridad administrativa independiente»

1. Esta petición de decisión prejudicial versa, en síntesis, sobre las condiciones a las que deben atenerse las autoridades policiales para acceder a los datos almacenados en el teléfono móvil de la persona contra la que se dirige una investigación penal.

2. Como trataré de explicar, el reenvío prejudicial presenta notables deficiencias en cuanto a su admisibilidad. Si el Tribunal de Justicia decidiera, pese a todo, entrar en el fondo, habrá de pronunciarse sobre los ámbitos de aplicación respectivos de la Directiva 2002/58/CE [2] y de la Directiva (UE) 2016/680. [3]

[1] Lengua original: español.

[2] Directiva 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).

[3] Directiva del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DO 2016, L 119, p. 89).

I. Marco normativo

A. Derecho de la Unión

1. Reglamento (UE) 2016/679[4]

3. El artículo 2 («Ámbito de aplicación material»), apartado 2, establece:

«El presente Reglamento no se aplica al tratamiento de datos personales:

[…]

d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención».

2. Directiva 2016/680

4. En el considerando segundo se afirma:

«Los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales deben […] respetar sus libertades y derechos fundamentales, en particular el derecho a la protección de los datos personales. La presente Directiva pretende contribuir a la consecución de un espacio de libertad, seguridad y justicia».

5. El considerando cuadragésimo sexto enuncia:

«Toda restricción de los derechos del interesado debe cumplir con lo dispuesto en la Carta y el CEDH, según los ha interpretado la jurisprudencia del Tribunal de Justicia y del Tribunal Europeo de Derechos Humanos,[5] respectivamente, y, en particular, respetar el contenido esencial de los citados derechos y libertades».

6. En el considerando cuadragésimo nono se lee:

«Cuando los datos personales sean tratados en el transcurso de una investigación penal o un procedimiento judicial en materia penal, el ejercicio de los derechos de información, acceso a los datos personales, rectificación o supresión de estos y la limitación de su tratamiento podrá ejercerse de conformidad con el derecho procesal nacional».

7. El artículo 1 («Objeto y objetivos») dispone:

«1. La presente Directiva establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales por parte de las autoridades competentes, con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de

4 Reglamento 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). En lo sucesivo, «RGPD».

5 En lo sucesivo, «TEDH».

ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.

2. De conformidad con la presente Directiva, los Estados miembros deberán:

a) proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales, y

[…]

3. La presente Directiva no impedirá a los Estados miembros ofrecer mayores garantías que las que en ella se establecen para la protección de los derechos y libertades del interesado con respecto al tratamiento de datos personales por parte de las autoridades competentes».

8. El artículo 2 («Ámbito de aplicación»), apartado 1, recoge:

«La presente Directiva se aplica al tratamiento de datos personales por parte de las autoridades competentes a los fines establecidos en el artículo 1, apartado 1».

9. El artículo 3 («Definiciones») estipula:

«A efectos de la presente Directiva se entenderá por:

[…]

2) “tratamiento”: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

[…]

7) “autoridad competente”:

   a) toda autoridad pública competente para la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública, o

[…]».

10. El artículo 4 («Principios relativos al tratamiento de datos personales»), apartado 1, prescribe:

«Los Estados miembros dispondrán que los datos personales sean:

a) tratados de manera lícita y leal;

b) recogidos con fines determinados, explícitos y legítimos, y no ser tratados de forma incompatible con esos fines;

c) adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados;

[…]

e) conservados de forma que permita identificar al interesado durante un período no superior al necesario para los fines para los que son tratados;

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidentales, mediante la aplicación de medidas técnicas u organizativas adecuadas».

11. El artículo 8 («Licitud del tratamiento») indica:

«1. Los Estados miembros dispondrán que el tratamiento solo sea lícito en la medida en que sea necesario para la ejecución de una tarea realizada por una autoridad competente, para los fines establecidos en el artículo 1, apartado 1, y esté basado en el derecho de la Unión o del Estado miembro.

2. El derecho del Estado miembro que regule el tratamiento dentro del ámbito de aplicación de la presente Directiva, deberá indicar al menos los objetivos del tratamiento, los datos personales que vayan a ser objeto del mismo y las finalidades del tratamiento».

12. El artículo 13 («Información que debe ponerse a disposición del interesado o que se le debe proporcionar») prescribe:

«1. Los Estados miembros dispondrán que el responsable del tratamiento de los datos ponga a disposición del interesado al menos la siguiente información:

[…]

d) el derecho a presentar una reclamación ante la autoridad de control y los datos de contacto de la misma;

[…]

3. Los Estados miembros podrán adoptar medidas legislativas por las que se retrase, limite u omita la puesta a disposición del interesado de la información en virtud del apartado 2 siempre y cuando dicha medida constituya una medida necesaria y proporcional en una sociedad democrática, teniendo debidamente en cuenta los derechos fundamentales y los intereses legítimos de la persona física afectada, para:

a) evitar que se obstaculicen indagaciones, investigaciones o procedimientos oficiales o judiciales;

b) evitar que se cause perjuicio a la prevención, detección, investigación o enjuiciamiento de infracciones penales o a la ejecución de sanciones penales;

c) proteger la seguridad pública;

d) proteger la seguridad nacional;

e) proteger los derechos y libertades de otras personas.

[…]»

13. Conforme al artículo 15 («Limitaciones al derecho de acceso»), apartado 1:

«Los Estados miembros podrán adoptar medidas legislativas por las que se restrinja, total o parcialmente, el derecho de acceso del interesado siempre y cuando dicha restricción parcial o completa constituya una medida necesaria y proporcional en una sociedad democrática, teniendo debidamente en cuenta los derechos fundamentales y los intereses legítimos de la persona física afectada, para:

a) evitar que se obstaculicen indagaciones, investigaciones o procedimientos oficiales o judiciales;

b) evitar que se cause perjuicio a la prevención, detección, investigación o enjuiciamiento de infracciones penales o a la ejecución de sanciones penales;

c) proteger la seguridad pública;

d) proteger la seguridad nacional;

e) proteger los derechos y libertades de otras personas».

14. En virtud del artículo 27 («Evaluación de impacto relativa a la protección de datos»):

«1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, suponga un alto riesgo para los derechos y libertades de las personas físicas, los Estados miembros dispondrán que el responsable del tratamiento lleve a cabo, con carácter previo, una evaluación del impacto de las operaciones de tratamiento previstas en la protección de datos personales.

2. La evaluación mencionada en el apartado 1 incluirá, como mínimo, una descripción general de las operaciones de tratamiento previstas, una evaluación de los riesgos para los derechos y libertades de los interesados, las medidas contempladas para hacer frente a estos riesgos, y las garantías, medidas de seguridad y mecanismos destinados a garantizar la protección de los datos personales y a demostrar la conformidad con la presente Directiva, teniendo en cuenta los derechos e intereses legítimos de los interesados y las demás personas afectadas».

15. El artículo 28 («Consulta previa a la autoridad de control») proclama:

«1. Los Estados miembros velarán por que el responsable o el encargado del tratamiento consulte a la autoridad de control antes de proceder al tratamiento de datos personales que vayan a formar parte de un nuevo fichero que haya de crearse, cuando:

a) la evaluación del impacto en la protección de los datos que prevé el artículo 27 indique que el tratamiento entrañaría un alto riesgo a falta de medidas adoptadas por el responsable a fin de mitigar el riesgo, o

b) el tipo de tratamiento, en particular cuando se usen tecnologías, mecanismos o procedimientos nuevos, constituya un alto riesgo para los derechos y libertades de los interesados.

[…]».

16. El artículo 54 («Derecho a la tutela judicial efectiva contra el responsable o el encargado del tratamiento») establece:

«Sin perjuicio de los recursos administrativos o extrajudiciales disponibles, incluido el derecho a presentar una reclamación ante una autoridad de control con arreglo al artículo 52, los Estados miembros reconocerán el derecho que asiste a todo interesado a la tutela judicial efectiva si considera que sus derechos establecidos en disposiciones adoptadas con arreglo a la presente Directiva han sido vulnerados como consecuencia de un tratamiento de sus datos personales no conforme con esas disposiciones».

B. Derecho nacional

17. El artículo 18 de la Strafprozessordnung[6] asigna a la policía judicial funciones al servicio de la administración de justicia penal (apartado 1). Las investigaciones de la policía judicial serán responsabilidad de las autoridades de seguridad (apartado 2). Los órganos del servicio de seguridad pública prestarán el servicio ejecutivo de la policía judicial, que consiste en investigar y perseguir las infracciones penales (apartado 3).

18. Con arreglo al artículo 99 de la StPO, la policía judicial investiga de oficio o sobre la base de una denuncia, debiendo atenerse a las órdenes del Ministerio Fiscal y de los órganos jurisdiccionales (apartado 1). Cuando una medida de investigación requiera la orden del Ministerio Fiscal, la policía judicial puede ejercer la facultad correspondiente, aún sin tal orden, en caso de peligro inminente. En tal supuesto, debe solicitar inmediatamente la autorización (apartado 2).

19. De acuerdo con el artículo 111, apartado 2, de la StPO, cuando la información almacenada en soportes de datos deba ser objeto de una recogida de datos, toda persona está obligada a permitir el acceso a dicha información y, previa solicitud, a entregar o permitir la realización de un soporte de datos electrónico en un formato de archivo corrientemente utilizado. Además, debe permitir que se realice una copia de salvaguardia de la información almacenada en los soportes de datos.

II. Hechos, litigio y preguntas prejudiciales

20. C. G. es un ciudadano alemán que trabaja y reside en Austria.

21. El 23 de febrero de 2021, al realizar un control de estupefacientes, funcionarios de la oficina aduanera de Innsbruck (Austria) intervinieron un paquete dirigido a C. G. que contenía 85 gramos de cannabis.

22. El 6 de marzo de 2021, dos agentes de policía interrogaron a C. G. acerca del remitente del paquete y registraron su vivienda. En el curso de ese registro, se incautaron de su teléfono móvil (que incluía una tarjeta SIM y otra SD) y le entregaron el acta de la incautación.

[6] Código de procedimiento penal. En lo sucesivo, «StPO». BGBl nº 631/1975, en la versión aplicable en el momento de los hechos (BGBl I nº 24/2020).

23. Requerido para que permitiera el acceso a los datos de conexión de su teléfono móvil, C. G. se negó, así como a revelar el código de acceso al teléfono.

24. La oficina de policía del distrito de Landeck (Austria) no logró desbloquear el teléfono móvil. Este fue enviado a la Bundeskriminalamt (Oficina Central de Policía Judicial) en Viena (Austria), donde se intentó nuevamente, sin éxito, desbloquearlo y consultar los datos almacenados.

25. En el momento en el que fueron adoptadas por la policía, esas medidas no estaban cubiertas por una orden del Ministerio Fiscal ni por una resolución judicial.

26. El 31 de marzo de 2021, C. G. presentó un recurso ante el Landesverwaltungsgericht Tirol (Tribunal regional de lo contencioso administrativo del Tirol, Austria) contra la medida coercitiva que se le había impuesto, impugnando la incautación de su teléfono móvil. Este le fue devuelto el 20 de abril de 2021.

27. C. G. no fue informado de los intentos de analizar el contenido del teléfono móvil; tuvo conocimiento de ellos debido a que el agente de policía que procedió a la incautación y, posteriormente, inició el análisis digital fue interrogado como testigo sometido a la obligación de decir la verdad. Esos intentos tampoco se documentaron en el expediente de la policía judicial.

28. En este contexto, el Landesverwaltungsgericht Tirol (Tribunal regional de lo contencioso administrativo del Tirol) dirigió al Tribunal de Justicia las siguientes preguntas prejudiciales:

«1) ¿Debe interpretarse el artículo 15, apartado 1, de la Directiva 2002/58 (en su caso, en relación con su artículo 5), en su versión modificada por la Directiva 2009/136/CE, a la luz de los artículos 7 y 8 de la Carta […], en el sentido de que el acceso por las autoridades públicas a los datos almacenados en teléfonos móviles constituye una injerencia en los derechos fundamentales consagrados en dichos artículos de la Carta suficientemente grave como para que deba limitarse dicho acceso, en el ámbito de la prevención, la investigación, el descubrimiento y la persecución de delitos, a la lucha contra la delincuencia grave?

2) ¿Debe interpretarse el artículo 15, apartado 1, de la Directiva 2002/58, en su versión modificada por la Directiva 2009/136/CE, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, en el sentido de que se opone a una normativa nacional como el artículo 18 de la [StPO] en relación con el artículo 99, apartado 1, de esa misma Ley, que permite a las autoridades de seguridad obtener por sí mismas, en el marco de un procedimiento de investigación penal, sin autorización de un órgano jurisdiccional o de una autoridad administrativa independiente, un acceso completo e incontrolado a todos los datos digitales almacenados en un teléfono móvil?

3) ¿Debe interpretarse el artículo 47 de la Carta […] en su caso en relación con los artículos 41 y 52 de esta, en el sentido de que, desde el punto de vista de la igualdad de armas y de la tutela judicial efectiva, se opone a la normativa de un Estado miembro, como el artículo 18, de la [StPO] en relación con el artículo 99, apartado 1, de esa misma Ley, que permite el análisis digital de un teléfono móvil sin que el interesado sea informado previamente o, al menos, después de que se haya adoptado dicha medida?»

III. Procedimiento ante el Tribunal de Justicia

29. La petición de decisión prejudicial se registró en el Tribunal de Justicia el 6 de septiembre de 2021.

30. El 20 de octubre de 2021, el Tribunal de Justicia requirió al órgano judicial de remisión para que manifestara si la Directiva 2016/680 podría ser pertinente para el caso.

31. El 11 de noviembre de 2021, el tribunal de reenvío respondió que la Directiva 2016/680 debe ser aplicada en el litigio principal.

32. Han presentado observaciones escritas los Gobiernos alemán, austríaco, chipriota, danés, estonio, francés, húngaro, irlandés, neerlandés, noruego, polaco y sueco, así como la Comisión Europea.

33. En la vista pública, celebrada el 16 de enero de 2023, han comparecido, con la excepción de los Gobiernos alemán, húngaro y polaco, quienes habían presentado observaciones escritas, además del Gobierno finlandés. Todos ellos fueron invitados por el Tribunal de Justicia a concentrar sus alegaciones sobre la Directiva 2016/680 y a responder oralmente a determinadas preguntas en relación con esta.

IV. Análisis

A. Inadmisibilidad

34. El tribunal de reenvío formuló inicialmente sus preguntas demandando tan solo la interpretación de la Directiva 2002/58. Sin embargo, la práctica totalidad de quienes han intervenido en el procedimiento coinciden en que esa Directiva no se aplica a este asunto ni, en consecuencia, su interpretación resulta necesaria para zanjar el litigio.

35. A tenor de su artículo 3, la Directiva 2002/58 rige el «[…] tratamiento de datos personales en relación con la prestación de servicios de comunicaciones electrónicas disponibles al público en las redes públicas de comunicaciones de la [Unión], incluidas las redes públicas de comunicaciones que den soporte a dispositivos de identificación y recopilación de datos».

36. El Tribunal de Justicia ha declarado que «cuando los Estados miembros aplican directamente medidas que suponen excepciones a la confidencialidad de las comunicaciones electrónicas, sin imponer obligaciones de tratamiento a los proveedores de servicios de tales comunicaciones, la protección de los datos de las personas afectadas no está regulada por la Directiva 2002/58, sino únicamente por el derecho nacional, sin perjuicio de la aplicación de la [Directiva 2016/680]».[7]

37. En el asunto que ahora nos ocupa, la tentativa de acceso a los datos la realizaron directamente las autoridades policiales en el marco de una investigación penal. No hubo intervención de los proveedores de servicios de comunicaciones electrónicas, a quienes no se les requirió la comunicación de datos personales. No entra en juego, pues, la Directiva 2002/58.

[7] Sentencia de 6 de octubre de 2020, La Quadrature du Net y otros (C-511/18, C-512/18 y C-520/18, EU:C:2020:791; en lo sucesivo, «sentencia La Quadrature du Net»), apartado 103.

38. La norma del derecho de la Unión que rige esta situación es la Directiva 2016/680, en virtud de cuyo artículo 2, apartado 1, se aplica al tratamiento de datos personales por las autoridades competentes a los «fines de […] investigación […] de infracciones penales».

39. Lo anterior sería suficiente para inclinarse por la inadmisibilidad del reenvío prejudicial, tal como lo había formulado el órgano judicial nacional, pues la norma del derecho de la Unión cuya interpretación solicitaba no era aplicable al caso.

40. Es cierto, empero, que el artículo 267 TFUE permite al Tribunal de Justicia reformular las preguntas prejudiciales que se le plantean o indicar la existencia de otras normas del derecho de la Unión eventualmente pertinentes, a fin de proporcionar al órgano jurisdiccional nacional una respuesta útil. [8]

41. El Tribunal de Justicia se dirigió al de reenvío para que se pronunciara sobre la eventual incidencia de la Directiva 2016/680. Le brindó, pues, la posibilidad de que él mismo completara o reformulara sus preguntas. En vez de hacerlo así, el órgano de reenvío se ha limitado a manifestar que «en el presente asunto procede, en todo caso, respetar lo dispuesto en la Directiva 2016/680», pero sin identificar los preceptos de esta sobre los que tiene dudas ni extenderse en otras consideraciones de fondo. [9]

42. El Tribunal de Justicia ha declarado reiteradamente que «es indispensable, como dispone el artículo 94, letra c), del Reglamento de Procedimiento, que la petición de decisión prejudicial contenga la indicación de las razones que han llevado al órgano jurisdiccional remitente a preguntarse sobre la interpretación o la validez de determinadas disposiciones del derecho de la Unión, así como de la relación que a su juicio existe entre dichas disposiciones y la normativa nacional aplicable en el litigio principal». [10]

43. Pues bien, el incumplimiento de los requisitos del artículo 94 del Reglamento de Procedimiento es claro en este reenvío, a resultas de cuanto se ha expuesto. Aun cuando el Tribunal de Justicia hace gala de una cierta flexibilidad al respecto, la cooperación con el órgano judicial de reenvío ha de ser recíproca: en ausencia, injustificada, de una colaboración por parte de este para exponer sus dudas sobre la interpretación del derecho de la Unión que repute aplicable (en este caso, la Directiva 2016/680), me parece lógico inadmitir la petición de decisión prejudicial. [11]

44. A lo anterior se une que aquel tribunal:

— No ha precisado la naturaleza del tratamiento intentado por las autoridades policiales, o de los datos personales concretamente buscados. En un primer momento, parece indicar que se limitaba a datos de conexión (es decir, de tráfico y de localización), pero después no excluye que el desbloqueo del teléfono propiciase el acceso a «todos los datos digitales almacenados» [12]

[8] Por todas, sentencia de 28 de abril de 2016, Oniors Bio (C-233/15, EU:C:2016:305), apartado 30.

[9] El Tribunal de Justicia se vio en la necesidad de invitar a las partes a que señalasen «cuáles son, a su juicio, las disposiciones pertinentes de la Directiva 2016/680 a cuya luz el Tribunal debería, en su caso, reformular las tres preguntas prejudiciales planteadas por la jurisdicción de reenvío» (cuarta pregunta de las dirigidas para respuesta oral en la vista).

[10] Sentencia de 6 de octubre de 2021, Consorzio Italian Management y Catania Multiservizi (C-561/19, EU:C:2021:799), apartado 69.

[11] Coincido en esa apreciación con el Gobierno francés (apartados 36 a 41 de sus observaciones escritas).

[12] Así, en la segunda pregunta prejudicial.

e incluso al contenido de las comunicaciones y de los mensajes electrónicos intercambiados a través de él. [13]

— Alude tanto a la incautación del teléfono y al acceso, o tentativa de acceso, a los datos contenidos en él como a su subsiguiente «explotación» (*Auswertung*), esto es a su análisis y lectura. Esta última, añade, «implica un acceso completo e incontrolado a todas las comunicaciones digitales del interesado», lo que permite «reconstruir una imagen muy detallada y en profundidad de casi todos los ámbitos de la vida privada».

45. En estas condiciones, más que una *reformulación* de las preguntas del tribunal de origen, el Tribunal de Justicia llevaría a cabo una verdadera *reconstrucción* del reenvío prejudicial, basada, además, parcialmente en consideraciones hipotéticas, antes que en hechos acreditados. Todo eso, insisto, tras haber brindado al órgano judicial la posibilidad de completar o reformular por sí mismo sus preguntas.

46. Propugno, pues, que se declare inadmisible el reenvío prejudicial, como han instado varios de los Estados intervinientes.

47. A esa misma declaración de inadmisibilidad habría de conducir la circunstancia, destacada en la vista, de que ante el tribunal *a quo* no existe ya un verdadero litigio que requiera la interpretación de normas del derecho de la Unión.

48. En efecto, el Gobierno austríaco (del que dependen las autoridades policiales que intervinieron en la investigación) reconoce que la actuación de esas autoridades fue ilícita y vulneró los derechos del afectado. Como quiera que, según el auto de reenvío, la pretensión del recurrente ante la jurisdicción contencioso administrativa iba dirigida, justamente, contra las medidas policiales que la Administración demandada considera ilícitas, ha desaparecido la controversia sometida al juicio del tribunal de remisión.

49. En todo caso, por si el Tribunal de Justicia no compartiera mi parecer, me ocuparé en lo que sigue, con carácter subsidiario, de los problemas de fondo que subyacen en las preguntas prejudiciales.

50. Antes, sin embargo, me parece necesario descartar la concurrencia de otro motivo de inadmisibilidad esgrimido por algunos de los intervinientes en el procedimiento. [14] A su entender, como la Directiva 2016/680 atiende a la protección de las personas físicas en lo que atañe al *tratamiento* de sus datos, no regiría supuestos como este, donde no habría habido tratamiento, sino una simple *tentativa de acceso* a datos que no pudieron finalmente ser obtenidos.

51. Para la Comisión, por el contrario, el efecto útil de la Directiva 2016/680 debería privilegiar una interpretación de su objeto que no se limitara al tratamiento de datos en sentido estricto, sino que comprendiera también cuestiones que le estén directamente vinculadas. Una de estas últimas sería la tentativa de acceder a los datos cuyo tratamiento se pretende. [15]

[13] Afirma el tribunal de renvío que «por lo que respecta a los datos de conexión, se pueden reconstruir casi todos los contactos, según la frecuencia, el tiempo y la duración de las comunicaciones; por lo que respecta a las comunicaciones efectuadas a través de SMS y de otros servicios de mensajería de texto también se puede reconstituir el contenido; asimismo, el análisis de fotografías e historiales de navegación almacenados aporta un conocimiento muy íntimo de la vida privada del interesado».

[14] Me refiero, concretamente, a los Gobiernos austriaco, francés, neerlandés y noruego.

[15] Para la Comisión, «es indiferente que las tentativas se hayan visto coronadas por el éxito o no. La aparición de dificultades técnicas que impiden el éxito de las tentativas de acceso es una circunstancia que no puede conocerse con antelación y que no afecta a los riegos para la protección de los datos personales».

52. A mi juicio, sin necesidad de forzar los límites del ámbito de la Directiva 2016/680,[16] su aplicación a este supuesto se justifica no porque se haya producido la incautación del teléfono móvil,[17] sino por la actuación subsiguiente de las autoridades policiales para obtener de él ciertos datos personales del interesado, a cuyo fin intentaron desbloquearlo y habilitar el acceso a su contenido.

53. Entre las operaciones definidas como «tratamiento» por el artículo 3, punto 2, de la Directiva 2016/680 se halla «cualquier otra forma de habilitación de acceso» a los datos personales, realizada en el curso de una investigación penal. Entiendo que, cuando la autoridad policial incauta un teléfono donde se conservan esos datos y lo manipula para extraerlos de él, inicia una «operación» de tratamiento, por más que se frustre debido a razones técnicas concernientes a la seguridad criptográfica.

54. Una tentativa frustrada de acceso a los datos personales conservados en un teléfono móvil, en una investigación penal, se rige por la Directiva 2016/680 por análogas razones a las que determinaron que el Tribunal de Justicia declarara aplicable la Directiva 2002/58 al *intento* (asimismo frustrado) de obtener la autorización judicial para acceder a ciertos datos de la persona investigada, que se hallaban en poder de un operador de comunicaciones electrónicas.[18]

55. En ese contexto, si el tribunal de reenvío hubiera de pronunciarse sobre la ilicitud de la actuación policial (reconocida por el Gobierno austriaco, según ya he expuesto), su apreciación podría depender de la legalidad del fin que con ella se pretendiese, tanto si la medida tuvo éxito como si solo se empezó, infructuosamente, a ejecutar.

B. Sobre el fondo

1. Primera pregunta prejudicial

56. El tribunal *a quo* quiere saber si, con arreglo al artículo 15, apartado 1, de la Directiva 2002/58 (en su caso, en relación con su artículo 5) y a la luz de los artículos 7 y 8 de la Carta, «el acceso por las autoridades públicas a los datos almacenados en teléfonos móviles constituye una injerencia en los derechos fundamentales consagrados en dichos artículos de la Carta suficientemente grave como para que deba limitarse dicho acceso, en el ámbito de la prevención, la investigación, el descubrimiento y la persecución de delitos, a la lucha contra la delincuencia grave».

57. De ser admisible el reenvío, la inaplicabilidad de la Directiva 2002/58 obligaría a reformular el primer interrogante, de modo que la respuesta del Tribunal de Justicia interpretase la Directiva 2016/680.

[16] Me parece, en particular, innecesario el recurso a los artículos 27 y 28 de la Directiva 2016/680, sugerido por la Comisión en sus observaciones escritas. La «evaluación de impacto relativa a la protección de datos» establecida por el artículo 27 se refiere, genéricamente, a «un tipo de tratamiento» y no a tratamientos concretos o particulares. Así se desprende del considerando quincuagésimo octavo de la Directiva 2016/680: «[l]as evaluaciones de impacto deben abarcar los sistemas y procesos correspondientes de las operaciones de tratamiento, pero *no harán referencia a casos concretos*» (cursiva añadida). La Comisión matizó en la vista su invocación de ambos preceptos, que habría citado solo para destacar cómo la Directiva 2016/680 también contempla situaciones previas al tratamiento de datos propiamente dicho.

[17] La Directiva 2016/680 no regula la aprehensión del teléfono en cuanto medio de prueba en el marco de una investigación penal.

[18] Sentencia de 2 de octubre de 2018, Ministerio Fiscal (C-207/16, EU:C:2018: 788).

58. Esa respuesta debería aclarar, sucesivamente, si puede hablarse de injerencia en casos como el de autos y, de existir injerencia, si la Directiva 2016/680 exige que el acceso a los datos se circunscriba a los supuestos de lucha contra la delincuencia grave.

59. Las operaciones de tratamiento de datos pueden comprometer, por definición, los derechos al respeto de la vida privada (artículo 7 de la Carta) y a la protección de los datos de carácter personal (artículo 8 de la Carta). Las autoridades públicas, en consecuencia, han de ajustarse a las condiciones previstas en el artículo 52, apartado 1, de la Carta para justificar su intrusión en el ejercicio de esos derechos fundamentales.

60. La intrusión en los derechos protegidos por los artículos 7 y 8 de la Carta será tanto mayor cuanto que, con ella: a) se pretenda el acceso a datos de naturaleza sensible que usualmente se registran en los teléfonos móviles y cuyo conocimiento puede revelar facetas de la vida de sus titulares que deben quedar al abrigo del conocimiento de terceros; y b) se posibilite el acceso al contenido de las comunicaciones.

61. Ahora bien, desde una perspectiva general y habida cuenta de su contenido, no cabe interpretar la Directiva 2016/680 en el sentido de que los tratamientos de datos a los que se refiere se circunscriben únicamente a los supuestos de lucha contra la delincuencia grave.

62. La Directiva 2016/680 tiene por objeto cualquier operación de tratamiento [19] de datos personales por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de *todo tipo* de infracciones penales.

63. De los principios que la Directiva 2016/680 instaura en torno al tratamiento de datos personales con aquella finalidad (artículo 4), o de las condiciones de licitud para llevarlo a cabo (artículo 8), no se desprende que, como regla, el tratamiento de los datos solo sea viable en las hipótesis de criminalidad grave.

64. Una limitación constreñida a los supuestos de la lucha contra la delincuencia grave tampoco podría fundamentarse en la extrapolación, sin más, de la jurisprudencia del Tribunal de Justicia en relación con la Directiva 2002/58 [20] a supuestos como el de autos.

65. No puede hacerlo, a mi juicio, porque, sin perjuicio de lo que ulteriormente expondré, esa jurisprudencia se refiere a la conservación generalizada e indiscriminada de datos personales de un colectivo genérico e indeterminado, realizada por los proveedores de servicios de comunicaciones electrónicas con carácter sistemático. La magnitud de la injerencia que ese tipo de conservación supone para la sociedad en su conjunto explica que el Tribunal de Justicia se haya mostrado especialmente riguroso al proscribirla y contemplar las excepciones a esa prohibición.

66. No sucede así cuando el acceso pretendido no afecta al conjunto o a grandes grupos de la población (esto es, a los datos personales de un colectivo genérico e indeterminado), sino a la información almacenada en un teléfono móvil singular, en el marco de un procedimiento de investigación penal asimismo singular, para el que rige, específicamente, la Directiva 2016/680.

[19] La tipología de «operaciones» recogidas en el artículo 3, punto 2, de la Directiva 2016/680 es muy amplia. Véase su transcripción en el punto 9 de estas conclusiones.

[20] Sentencias La Quadrature du Net y de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C-203/15 y C-698/15, EU:C:2016:970; en lo sucesivo, «sentencia Tele2 Sverige y Watson»); de 2 de octubre de 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788); de 6 de octubre de 2020, Privacy International (C-623/17, EU:C:2020:790); y 2 de marzo de 2021, Prokuratuur (Condiciones de acceso a los datos relativos a las comunicaciones electrónicas) (C-746/18, EU:C:2021:152; en lo sucesivo, «sentencia Prokuratuur»).

67. El objeto de la Directiva 2016/680 no es otro que el tratamiento de datos por parte de las autoridades competentes para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales. De toda suerte de infracciones penales, y no únicamente de las de carácter grave.

68. Por lo demás, como han subrayado algunos de los intervinientes en el procedimiento prejudicial, a falta de cualquier indicación sobre la gravedad de las infracciones penales en la Directiva 2016/680, esta podría no aplicarse de un modo uniforme en los Estados miembros, pues las apreciaciones de cada derecho nacional sobre la mayor o menor gravedad de una conducta sancionable difieren sensiblemente. [21]

69. La Directiva 2016/680 no impone, en suma, como condición de licitud que el tratamiento de datos personales en ella regulado solo sea viable para la lucha contra la delincuencia grave.

70. Lo anterior no obsta a que, en aplicación del principio de proporcionalidad y caso por caso, el tratamiento de datos que las autoridades competentes pretendan hacer al amparo de la Directiva 2016/680 deba atemperarse en función de: a) la naturaleza de las infracciones penales perseguidas; y b) la cualidad de los datos personales a los que ese tratamiento se dirija.

71. Comparto, en esa línea, algunas afirmaciones del Gobierno alemán sobre la limitación del acceso a los datos de los teléfonos aprehendidos, cuando permitan establecer un perfil completo de la personalidad de sus titulares, a la vista del contenido digital de aquellos. Para el Gobierno alemán, ese acceso debería limitarse a los datos que sean necesarios como medio de prueba en un supuesto concreto y podría no ser adecuado ante factores como «el carácter menor de la infracción objeto de la investigación o el débil valor probatorio de los datos que se pretenden obtener». [22]

72. En *abstracto*, pues, la Directiva 2016/680 no implica que sea ilícito, por sistema, el acceso a los datos personales almacenados en un teléfono móvil con el propósito de facilitar la investigación sobre conductas que puedan englobarse en la criminalidad general o común. Si, *en concreto*, procede ese acceso, será algo que la autoridad correspondiente habrá de valorar en cada ocasión, atendiendo a su necesidad y al criterio de proporcionalidad al que me acabo de referir.

73. Así se deduce, en mi opinión, de los preceptos de la Directiva 2016/680 que establecen las condiciones de validez de los tratamientos de datos personales en el marco de la lucha contra la delincuencia:

— El artículo 4, apartado 1, letra a), en cuya virtud los datos han de ser «tratados de manera lícita».

— El artículo 8, apartado 1, en el que se destaca que el tratamiento ha de resultar *necesario* y basarse en el derecho de la Unión o del Estado miembro.

[21] El Gobierno francés pone como ejemplo las infracciones en materia de posesión y tráfico de drogas, sobre cuya gravedad difieren las normas penales de Austria y Francia. En análogo sentido se pronuncia el Gobierno sueco.

[22] Observaciones escritas del Gobierno alemán, apartado 20.

2. Segunda pregunta prejudicial

74. Con su segunda pregunta prejudicial, el tribunal de reenvío quiere saber si el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta «se opone a una normativa nacional como el artículo 18 de la [StPO] en relación con el artículo 99, apartado 1, de esa misma Ley, que permite a las autoridades de seguridad obtener por sí mismas, en el marco de un procedimiento de investigación penal, sin autorización de un órgano jurisdiccional o de una autoridad administrativa independiente, un acceso completo e incontrolado a todos los datos digitales almacenados en un teléfono móvil».

75. La redacción de la pregunta incurre en una cierta ambigüedad. El tribunal de reenvío:

— Reconoce que el artículo 110, apartado 2, de la StPO prevé que las incautaciones de bienes requieran, en principio, la autorización del Ministerio Fiscal. La autoridad policial sólo puede proceder a esas incautaciones, sin tal autorización, en las hipótesis extraordinarias previstas en el apartado 3 de ese mismo artículo (que no parecen concurrir en este caso).

— Añade, sin embargo, que el análisis de las informaciones almacenadas en los teléfonos móviles «no está reglamentado [en la StPO] de forma unívoca» y que podrían llevarlo a cabo las autoridades de seguridad por su propia iniciativa, sin previa autorización.

76. El Gobierno austriaco ofrece una versión de la normativa nacional que no se compadece con la que expone el auto de reenvío. En particular, afirma que, con arreglo al derecho nacional, tanto la incautación del teléfono (a salvo los supuestos de urgencia) como el análisis de los datos en él almacenados solo es posible mediando autorización del Ministerio Fiscal.[23] Sin una orden del Ministerio Fiscal, la explotación policial de los datos conservados en ese teléfono es ilícita.

77. Corresponde al tribunal de remisión verificar los términos de la normativa interna. En el marco del procedimiento previsto en el artículo 267 TFUE, el Tribunal de Justicia no es competente para interpretar el derecho nacional, y es el juez de reenvío, en exclusiva, quien ha de definir el alcance exacto de las disposiciones legales, reglamentarias y administrativas nacionales.[24]

78. Sin ánimo de terciar en la polémica sobre la interpretación del derecho austríaco, me parece difícil inferir de los solos preceptos que el tribunal de reenvío identifica (artículo 18 de la StPO en relación con el artículo 99, apartado 1, de la misma ley) la consecuencia que él mismo deduce. Pero, repito, eso es algo que solo aquel tribunal puede resolver.

79. Sea como fuere, el tribunal de reenvío considera que sería trasladable a un supuesto como el de autos la doctrina de la sentencia Prokuratuur,[25] sobre el control previo, por parte de un órgano jurisdiccional o de una autoridad independiente, del acceso a los datos conservados.

[23] Apartado 19 del escrito de observaciones del Gobierno austríaco. Cita la decisión del Oberster Gerichtshof (Tribunal Supremo, Austria) de 13 de octubre de 2020 (asunto 11 Os 56/20z) que califica de ilícito, en cuanto vulnerador de los derechos subjetivos del afectado, el análisis por la policía judicial de los datos de un teléfono móvil sin contar con la autorización del Ministerio Fiscal.

[24] Por todas, sentencia de 28 de abril de 2022, SeGEC y otros (C-277/21, EU:C:2022:318), apartado 21.

[25] Sentencia Prokuratuur, apartado 51: «es esencial que el acceso de las autoridades nacionales competentes a los datos conservados se supedite a un control previo efectuado bien por un órgano jurisdiccional, bien por una entidad administrativa independiente, y que la decisión de este órgano jurisdiccional o de esta entidad se dicte a raíz de una solicitud motivada de dichas autoridades presentada, en particular, en el marco de procedimientos de prevención, descubrimiento y persecución de delitos».

80. Para el Gobierno neerlandés, por el contrario, esa doctrina ha de entenderse en el contexto de una normativa nacional que permitía el acceso *general* de las autoridades competentes a *todos* los datos de tráfico y de localización conservados. Así se explicaría el requerimiento de una previa autorización judicial que podría no justificarse, sin embargo, en el caso del acceso a los datos de un único teléfono móvil.

81. En esa misma línea, el Gobierno noruego alega, que entre las múltiples garantías establecidas por la Directiva 2016/680 [26] no figura explícitamente la de la necesidad de una previa autorización a cargo de una autoridad judicial o administrativa independiente.

82. La Comisión, partiendo de que las disposiciones de la Directiva 2016/680 deben interpretarse a la luz de la Carta, alega que la obligación impuesta a los Estados miembros en el artículo 8, apartado 1, de esa Directiva (condiciones de licitud del tratamiento) comporta la necesidad de respetar los derechos fundamentales garantizados por los artículos 7 y 8 de la Carta.

83. Coincido con la Comisión en que, respetando esos preceptos de la Carta, los legisladores nacionales están obligados a definir las reglas necesarias para garantizar que el acceso a los datos esté justificado en cada caso y se limite a lo que resulte estrictamente necesario y proporcionado.

84. Tales reglas nacionales, sin embargo, no tienen por qué ser específicas para el acceso a los datos personales contenidos, como aquí ocurre, en un teléfono móvil, sino que pueden ser las previstas en el derecho interno, con carácter general, en materia de obtención de pruebas.

85. A este respecto ya he transcrito el apartado 103 de la sentencia La Quadrature du Net en cuanto a las medidas de los Estados miembros que afectan a la confidencialidad de las comunicaciones electrónicas, sin imponer obligaciones de tratamiento a los proveedores de servicios de tales comunicaciones. [27]

86. Sin necesidad, por tanto, de deducir de la Directiva 2016/680 reglas *específicas* de naturaleza procesal en garantía de la licitud del acceso a los datos almacenados en un teléfono móvil, [28] se aplicarán las normas nacionales que regulan el ejercicio de los poderes de registro e incautación en el marco de las investigaciones penales. [29]

87. La remisión a las disposiciones del derecho interno para garantizar la licitud del acceso con arreglo a la Directiva 2016/680 está, por lo demás, en consonancia con la jurisprudencia del TEDH. Precisamente en un supuesto referido a la República de Austria en relación con el artículo 8 CEDH (derecho al respeto de la vida privada y familiar, así como del domicilio y de la correspondencia) el TEDH constató que la legislación austriaca sobre la incautación de objetos y, en particular, de documentos, se aplica al registro y a la incautación de datos conservados en soportes informáticos. [30]

[26] Además de las de los artículos 4 y 8, las contenidas en los capítulos III («Derechos del interesado»), IV («Responsable del tratamiento y encargado del tratamiento»), VI («Autoridades de control independiente») y VIII («Recursos, responsabilidad y sanciones»).

[27] Véase el punto 36 de estas conclusiones.

[28] Empresa de cuya dificultad son buena muestra los esfuerzos de la Comisión en los apartados 34 a 39 de su escrito de observaciones por contribuir a la definición de reglas claras y precisas para la configuración de los límites y de las garantías adecuadas en relación con el acceso a los datos de un teléfono móvil.

[29] Normas que, como recuerdan, por ejemplo, los Gobiernos danés e irlandés, están fuera del ámbito de aplicación del derecho de la Unión, pero que pueden servir a la satisfacción de una exigencia resultante de aquel derecho.

[30] Sentencia del TEDH de 16 de octubre de 2007, Wieser y Bicos Beteiligungen c. Austria (CE:ECHR:2007:1016JUD007433601), § 54: «the Austrian Code of Criminal Procedure does not contain specific provisions for the search and seizure of electronic data. However, it contains detailed provisions for the seizure of objects and, in addition, specific rules for the seizure of documents. It is established in the domestic courts' case-law that these provisions also apply to the search and seizure of electronic data».

88. Si, como sostiene el Gobierno austríaco con cita de la jurisprudencia del Oberster Gerichtshof (Tribunal Supremo, Austria), las autoridades policiales no están legitimadas para acceder a los datos guardados en un determinado teléfono móvil sin autorización del Ministerio Fiscal, la segunda pregunta prejudicial pierde buena parte de su sentido.

89. En cualquier caso, la respuesta a esa pregunta no puede descartar que el acceso a los datos personales del teléfono incautado conduzca a «reconstruir una imagen muy detallada y en profundidad de casi todos los ámbitos de la vida privada» del interesado.[31] De ser así, las autoridades policiales no podrían prescindir de la autorización previa a la que aludía la sentencia Prokuratuur.

90. A primera vista, esta afirmación parecería no casar con la inaplicación a este supuesto de la Directiva 2002/58 (que interpreta la sentencia Prokuratuur), tal como he defendido anteriormente. Entiendo, sin embargo, que la *ratio* de esta sentencia abona la misma solución.

91. En el litigio que dio lugar a la sentencia Prokuratuur, aunque el acceso se llevó a cabo obteniendo los datos (metadatos) de los proveedores de servicios de comunicaciones electrónicas, estaba en juego, como aquí, una investigación penal singular, dirigida contra una persona determinada. Se trataba de recabar «datos relativos a varios números de teléfono de […] y a distintas identidades internacionales del equipo móvil de esta».[32]

92. En la sentencia Prokuratuur pueden distinguirse, a mi juicio, dos planos: a) el que pone en entredicho la normativa general de un Estado miembro sobre la conservación generalizada e indiferenciada y el ulterior acceso a los datos en poder de los proveedores del servicio; y b) el del control previo, para un caso singular, del acceso a esos metadatos, cuando permitan configurar un perfil preciso de la vida privada de una persona.

93. La circunstancia de que, en el asunto que ahora nos ocupa, los datos reveladores de la vida privada no estén en poder de los proveedores de servicio y se obtengan (o se traten de obtener) de un único teléfono incautado me parece de importancia secundaria frente a la *ratio* de la exigencia de control previo a la que apela la sentencia Prokuratuur.

94. Este control previo tiene su fundamento último en la protección que garantizan los artículos 7 y 8 de la Carta. La autoridad que lo lleve a cabo debe estar «en condiciones de ponderar adecuadamente, por una parte, los intereses relacionados con las necesidades de la investigación en el marco de la lucha contra la delincuencia y, por otra parte, los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales de aquellos a cuyos datos afecte el acceso».[33]

3. Tercera pregunta prejudicial

95. Con la tercera pregunta prejudicial el tribunal *a quo* desea saber si el artículo 47 de la Carta (en su caso, en relación con los artículos 41 y 52) se opone a una legislación como la austríaca[34] que «permite el análisis digital de un teléfono móvil sin que el interesado sea informado previamente o, al menos, después de que se haya adoptado dicha medida».

[31] Véanse las afirmaciones del tribunal de reenvío transcritas en el punto 44 de estas conclusiones.

[32] Sentencia Prokuratuur, apartado 17.

[33] Sentencia Prokuratuur, apartado 52.

[34] De nuevo se refiere al artículo 18 de la StPO en relación con su artículo 99.

96. Estimo que el interrogante redactado en esos términos podría resultar innecesario para resolver la controversia, porque el interesado pudo ejercer el derecho consagrado en el artículo 47 de la Carta, instando al tribunal de remisión a que declarase la nulidad de la acción policial sobre el teléfono incautado, que incluía la ulterior (y frustrada) explotación de los datos en él conservados.

97. En relación con esos dos momentos de la actuación policial, habría que distinguir:

— En cuanto a la incautación del teléfono en sí, las informaciones que obran en los autos revelan que el interesado tuvo conocimiento de ella y que se negó a facilitar a las autoridades policiales el código de desbloqueo cuando lo aprehendieron.

— En cuanto al intento de análisis de los datos, todo parece indicar que el responsable de tratamiento no informó al interesado de esa operación, aunque el Gobierno austriaco afirma que este último conoció un informe en el que se hacía constar la actuación de la policía judicial sobre el teléfono. [35]

98. Subsisten, pues, en torno a la explotación de los datos y a su conocimiento por el interesado ciertas ambigüedades que, como ya apunté, debería haber aclarado el tribunal *a quo* en el auto de reenvío y que impiden dar una respuesta útil a la tercera pregunta prejudicial.

99. En todo caso, por si el Tribunal de Justicia no reputara inadmisible esta pregunta, me pronunciaré sobre ella. En esa hipótesis, y dada la inaplicabilidad de la Directiva 2002/58, habría que reformularla a la luz de la Directiva 2016/680, cuyos artículos 13, 15 y 54 facilitan las pistas para responderla.

100. Con arreglo a la Directiva 2016/680, la información sobre el tratamiento de sus datos que debe facilitarse al interesado es la que resulte necesaria, entre otros extremos, para: a) presentar una reclamación ante la autoridad de control [artículo 13, apartado 1, letra d)]; y b) obtener la tutela efectiva de los tribunales frente a la vulneración de los derechos garantizados por la Directiva 2016/680, sin perjuicio de los recursos administrativos o extrajudiciales disponibles (artículo 54).

101. No cabe olvidar, sin embargo, que tanto el artículo 13, apartado 3, como el artículo 15, apartado 1, de la Directiva 2016/680 autorizan a los Estados miembros a adoptar medidas legislativas por las que:

— Se retrase, limite u omita la puesta a disposición del interesado de la información en virtud del apartado 2 del artículo 13.

— Se restrinja, total o parcialmente, el derecho de acceso del interesado a los datos tratados, siempre y cuando esa restricción constituya una medida necesaria y proporcional para, *inter alia*, evitar que se obstaculicen investigaciones o procedimientos oficiales o judiciales o se cause perjuicio a la investigación de infracciones penales. [36]

[35] Apartado 37 de su escrito de observaciones escritas.

[36] En este sentido, véase la sentencia Tele2 Sverige y Watson, apartado 121. Su doctrina en relación con la Directiva 2002/58 resulta trasladable a la Directiva 2016/680 en el contexto de la garantía de la tutela judicial de los derechos de los titulares de datos objeto de tratamiento.

102. De cualquier modo, la licitud del tratamiento de los datos no depende del cumplimiento por las autoridades competentes de los deberes (ulteriores) que les impone el artículo 13 de la Directiva 2016/680, sino de la legalidad del fin que lo haya justificado; es decir, de que esas autoridades administrativas estuvieran legitimadas para proceder al tratamiento de los datos personales.

103. Desde esa perspectiva, que el interesado haya sido informado de las tentativas de acceso a los datos almacenado en el teléfono que se le incautó es algo ajeno, en sí mismo, a la licitud por motivos sustantivos de la acción policial. La conducta del responsable del tratamiento eventualmente contraria a los deberes que le impone el artículo 13 de la Directiva 2016/680 podrá tener otras consecuencias, pero, repito, no afecta de suyo a la licitud o ilicitud de ese mismo tratamiento.

104. Corresponde al tribunal de reenvío determinar si la normativa nacional permite el ejercicio eficaz de aquellos derechos por parte de la persona afectada.

V. Conclusión

105. A tenor de lo expuesto, propongo al Tribunal de Justicia declarar inadmisible la petición de decisión prejudicial planteada por el Landesverwaltungsgericht Tirol (Tribunal de lo contencioso administrativo regional del Tirol, Austria).

Con carácter subsidiario, sugiero responder a esa petición en estos términos:

«1) Los artículos 4, apartado 1, letra a), y 8, apartado 1, de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, en relación con los artículos 7, 8, y 52 de la Carta de los Derechos Fundamentales de la Unión Europea,

han de interpretarse en el sentido de que

en el marco de una investigación penal, el acceso por las autoridades públicas a los datos personales almacenados en un teléfono móvil, con vistas a su tratamiento, no está limitado a los supuestos de lucha contra la delincuencia grave.

El referido acceso ha de estar justificado en cada caso y limitarse a lo que resulte estrictamente necesario y proporcionado, en función de la naturaleza de las infracciones penales perseguidas y de los datos personales a los que se pretenda acceder.

Las autoridades policiales no pueden obtener, por sí mismas y sin previa autorización de un órgano judicial, en el marco de una investigación penal, el acceso completo e incontrolado a todos los datos almacenados en un teléfono móvil, cuando de ellos se pueda obtener una imagen precisa de la vida privada de una persona.

2) Los artículos 13, 15 y 54 de la Directiva 2016/680, en relación con los artículos 47 y 52 de la Carta,

han de interpretarse en el sentido de que

sin perjuicio de las limitaciones autorizadas por el artículo 15, apartado 1, de la Directiva 2016/680, o de otros recursos administrativos o extrajudiciales disponibles, el titular de un teléfono móvil debe ser informado del tratamiento de los datos personales almacenados en él que hayan efectuado las autoridades correspondientes, en el momento y en los términos que resulten necesarios para garantizar el ejercicio efectivo de su derecho a recabar la tutela judicial frente a la eventual vulneración de los derechos reconocidos por la Directiva 2016/680».