



Recopilación de la Jurisprudencia

CONCLUSIONES DEL ABOGADO GENERAL
SR. GIOVANNI PITRUZZELLA
presentadas el 21 de enero de 2020¹

Asunto C-746/18

**H. K.
contra
Prokuratuur**

[Petición de decisión prejudicial planteada por el Riigikohus (Tribunal Supremo, Estonia)]

«Procedimiento prejudicial — Tratamiento de datos personales en el sector de las comunicaciones electrónicas — Confidencialidad de las comunicaciones — Proveedores de servicios de comunicaciones electrónicas — Conservación generalizada e indiferenciada de los datos de tráfico y de localización — Investigaciones penales — Acceso de la autoridad investigadora a los datos conservados correspondientes a períodos de entre un día y un año de duración — Autorización concedida por el Ministerio Fiscal — Utilización de los datos como prueba en el proceso penal — Directiva 2002/58/CE — Artículos 1, apartado 3, 3 y 15, apartado 1 — Carta de los Derechos Fundamentales de la Unión Europea — Artículos 7, 8 y 11 y artículo 52, apartado 1»

I. Introducción

1. La presente petición de decisión prejudicial tiene por objeto la interpretación del artículo 15, apartado 1, de la 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),² en su versión modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009,³ interpretado a la luz de los artículos 7, 8 y 11, así como del artículo 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea.⁴

2. Esta petición se ha presentado en el contexto de un procedimiento penal incoado contra H. K. por la presunta comisión de varios robos, la utilización de una tarjeta bancaria perteneciente a otra persona y la comisión de actos constitutivos de ataques a la libertad de los intervinientes en el proceso.

3. Los atestados en los que se fundamenta la apreciación de tales delitos fueron redactados principalmente basándose en datos personales generados en la prestación de servicios de comunicaciones electrónicas. El Riigikohus (Tribunal Supremo, Estonia) expresa sus dudas acerca de la compatibilidad con el Derecho de la Unión de las condiciones en las que tuvieron acceso a dichos datos los servicios de investigación.

¹ Lengua original: francés.

² DO 2002, L 201, p. 37.

³ DO 2009, L 337, p. 11. En lo sucesivo, «Directiva 2002/58».

⁴ En lo sucesivo, «Carta».

4. Esas dudas se refieren, en primer lugar, a la cuestión de si el período para el cual tuvieron acceso a los datos los servicios de investigación es un criterio que permita evaluar la gravedad de la injerencia de dicho acceso en los derechos fundamentales de las personas afectadas.

5. En segundo lugar, el órgano jurisdiccional remitente desea averiguar si, habida cuenta de los distintos cometidos que el Prokuratuur (Ministerio Fiscal, Estonia) tiene encomendados en virtud de la legislación estonia, es una autoridad administrativa «independiente» en el sentido de la sentencia de 21 de diciembre de 2016, *Tele2 Sverige y Watson y otros*.⁵

II. Marco jurídico

A. Directiva 2002/58

6. Con arreglo al artículo 1, apartado 3, de la Directiva 2002/58, esta «no se aplicará a las actividades no comprendidas en el ámbito de aplicación del Tratado constitutivo de la Comunidad Europea, como las reguladas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea, ni, en cualquier caso, a las actividades que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dichas actividades estén relacionadas con la seguridad del mismo) [ni] a las actividades del Estado en materia penal».

7. Además, el artículo 15, apartado 1, de dicha Directiva, dispone que «los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en los artículos 5 y 6, en los apartados 1 a 4 del artículo 8 y en el artículo 9 de la presente Directiva, cuando tal limitación constituya una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo 13 de la Directiva 95/46/CE.^[6] Para ello, los Estados miembros podrán adoptar, entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado. Todas las medidas contempladas en el presente apartado deberán ser conformes con los principios generales del Derecho [de la Unión], incluidos los mencionados en los apartados 1 y 2 del artículo 6 del Tratado de la Unión Europea».

B. Derecho estonio

1. Ley de Comunicaciones Electrónicas

8. La elektroonilise side seadus (Ley de Comunicaciones Electrónicas),⁷ de 8 de diciembre de 2004, en la versión aplicable al litigio principal, dispone, en su artículo 111¹, titulado «Obligación de conservar datos»:

«[...]»

5 C-203/15 y C-698/15, en lo sucesivo, «sentencia *Tele2 Sverige y Watson y otros*», EU:C:2016:970, apartado 120 y punto 2 del fallo.

6 Directiva 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 (DO 1995, L 281, p. 31).

7 RT I 2004, 87, 593.

(2) Los proveedores de servicios de telefonía fija y móvil, así como de servicios de red de telefonía fija y móvil, estarán obligados a conservar los datos siguientes:

- 1) El número de la línea que efectúa la llamada, así como el nombre y la dirección del abonado.
- 2) El número de la línea que recibe la llamada, así como el nombre y la dirección del abonado.
- 3) Cuando se utilice un servicio suplementario, como el desvío o la transferencia de llamadas: el número marcado, así como el nombre y la dirección del abonado.
- 4) La fecha y hora del inicio y de la finalización de la llamada.
- 5) El servicio de telefonía fija o móvil utilizado.
- 6) La identidad internacional del abonado móvil («International Mobile Subscriber Identity» — IMSI) de las líneas que efectúan y reciben la llamada.
- 7) La identidad internacional del equipo móvil («International Mobile Equipment Identity» — IMEI) de las líneas que efectúan y reciben la llamada.
- 8) El identificador de celda al inicio de la llamada.
- 9) Datos que permiten fijar la localización geográfica de la celda, mediante referencia a su identificador de localización, durante el período en el que se conserven los datos.
- 10) En el caso de los servicios anónimos de pago por adelantado: la fecha y hora de la primera activación del servicio y la etiqueta de localización desde la que se haya activado el servicio.

[...]

(4) Los datos mencionados en los apartados 2 y 3 del presente artículo serán conservados durante un período de un año a partir del momento de la comunicación, si dichos datos fueron generados o tratados en el curso de la prestación de un servicio de comunicación. [...]

[...]

(11) Los datos mencionados en los apartados 2 y 3 del presente artículo serán entregados:

- 1) con arreglo al *kriminaalmenetluste seadustik* [(Ley de Enjuiciamiento Criminal),⁸] a la autoridad investigadora, a un organismo autorizado para realizar medidas de vigilancia, al Ministerio Fiscal y al órgano jurisdiccional;

[...]».

2. *Ley de Enjuiciamiento Criminal*

9. El artículo 17 de la Ley de Enjuiciamiento Criminal, en la versión aplicable al litigio principal, titulado «Partes en el procedimiento judicial», dispone, en su apartado 1:

«Son partes en el procedimiento judicial el Ministerio Fiscal [...]».

⁸ RT I 2003, 27, 166.

10. A tenor del artículo 30 de la Ley de Enjuiciamiento Criminal, titulado «El Ministerio Fiscal en los procedimientos penales»:

«(1) El Ministerio Fiscal dirige el procedimiento de instrucción, garantizando su legalidad y eficacia, y ejerce la acusación pública ante el órgano jurisdiccional.

(2) Las competencias del Ministerio Fiscal en un procedimiento penal son ejercidas en su nombre por un fiscal que actuará con independencia y que solo estará sometido a la ley.»

11. El artículo 90¹ de la Ley de Enjuiciamiento Criminal, titulado «Solicitud de datos a una empresa de comunicaciones», establece, en sus apartados 2 y 3:

«(2) La autoridad investigadora podrá, con la autorización del Ministerio Fiscal en el procedimiento de instrucción o del órgano jurisdiccional en el procedimiento judicial, solicitar a un proveedor de servicios de comunicaciones electrónicas los datos enumerados en el artículo 111¹, apartados 2 y 3, de la Ley de Comunicaciones Electrónicas que no se mencionan en el apartado 1 del presente artículo. En la autorización de la solicitud se indicará, con fechas exactas, el período para el que se pueden solicitar los datos.

(3) Conforme al presente artículo, los datos solamente podrán ser solicitados si ello resulta indispensable para alcanzar el objetivo del procedimiento penal.»

12. El artículo 211 de la Ley de Enjuiciamiento Criminal, titulado «Objetivo del procedimiento de instrucción», está redactado en los siguientes términos:

«(1) El objetivo del procedimiento de instrucción es reunir pruebas y establecer las demás condiciones para la apertura del juicio oral.

(2) Durante el procedimiento de instrucción, la autoridad investigadora y el Ministerio Fiscal esclarecerán las circunstancias de cargo y de descargo del investigado o acusado.»

3. *Ley del Ministerio Fiscal*

13. La prokuratuuriseadus (Ley del Ministerio Fiscal),⁹ de 22 de abril de 1998, en la versión aplicable al litigio principal, dispone, en su artículo 1, titulado «El Ministerio Fiscal»:

«(1) El Ministerio Fiscal es una autoridad sujeta a la responsabilidad del Justiitsministeeriumi [(Ministerio de Justicia, Estonia)], que participa en la planificación de las medidas de vigilancia necesarias para luchar contra la delincuencia y esclarecer los delitos, que dirige el procedimiento de instrucción, garantizando su legalidad y eficacia, y que ejerce la acusación pública ante el órgano jurisdiccional y cumple las demás tareas que le atribuya la ley.

(1¹) El Ministerio Fiscal ejercerá de manera independiente las funciones que le encomienda la normativa y actuará con arreglo a esta Ley, a las demás leyes y a los actos normativos aprobados sobre la base de dichas leyes.

[...]»

⁹ RT I 1998, 41, 625.

14. El artículo 2 de la Ley del Ministerio Fiscal, titulado, «El Fiscal», establece, en su apartado 2:

«El fiscal ejercerá sus funciones de manera independiente y actuará únicamente de conformidad con la ley y su conciencia.»

III. Hechos, procedimiento principal y cuestiones prejudiciales

15. Mediante resolución de 6 de abril de 2017, H. K. fue condenada por el Viru Maakohus (Tribunal de Primera Instancia de Viru, Estonia), a una pena de prisión de dos años por la comisión, durante el período comprendido entre el 4 de agosto de 2015 y el 1 de febrero de 2016, de ocho hurtos de productos de alimentación y de otros bienes materiales de un valor de entre 3 y 40 euros, y por la sustracción de cantidades de dinero en efectivo de entre 5,20 y 2 100 euros, por haber utilizado la tarjeta bancaria de otra persona para retirar dinero de un cajero automático, causándole un perjuicio de 3 941,82 euros, y por actos constitutivos de ataques a la libertad de los intervinientes en el proceso.¹⁰

16. La condena del Viru Maakohus (Tribunal de Primera Instancia de Viru) a H. K. por tales delitos se basó, entre otros, en varios atestados confeccionados a partir de datos relativos a comunicaciones electrónicas, a los que se refiere el artículo 111¹, apartado 2, de la Ley de Comunicaciones Electrónicas, recabados por la autoridad investigadora del proveedor de servicios de telecomunicaciones durante el procedimiento de instrucción, después de haber obtenido las autorizaciones al efecto de un fiscal del Viru Ringkonnaprokuratuur (Fiscalía de Distrito de Viru, Estonia), de conformidad con el artículo 90¹, apartado 2, de la Ley de Enjuiciamiento Criminal.

17. Así, el 2 de noviembre de 2015, un fiscal de la Fiscalía de Distrito de Viru autorizó a la autoridad investigadora para recabar de la empresa de telecomunicaciones los datos a los que se refiere el artículo 111¹, apartado 2, de la Ley de Comunicaciones Electrónicas, a fin de determinar, a partir de dos números de teléfono móvil de H. K., la transmisión de llamadas y mensajes, su duración, el modo en que se efectuó la transmisión, los datos personales y la localización de quien efectuó la llamada y de quien la recibió, todo ello en relación con el 21 de septiembre de 2015.

18. El 4 de noviembre de 2015, la autoridad investigadora redactó un atestado relativo a los datos recabados de la empresa de telecomunicaciones sobre la base de dicha autorización en el que se especificaban las antenas de telefonía móvil en cuyo ámbito de alcance se había utilizado el número de abonado usado por H. K. el 21 de septiembre de 2015, después de las 19.00. Con dicho atestado, además de con otras pruebas, el Ministerio Fiscal quería probar ante el órgano jurisdiccional que fue H. K. quien cometió el hurto el 21 de septiembre de 2015.

19. El 25 de febrero de 2016, un fiscal de la Fiscalía de Distrito de Viru concedió a la autoridad investigadora, a efectos de investigar un delito tipificado en el artículo 303, apartado 1, del Karistusseadustik (Código Penal),¹¹ una autorización para recabar de la empresa de telecomunicaciones los datos a los que se refiere el artículo 111¹, apartado 2, de la Ley de Comunicaciones Electrónicas, relativos a los siete números de abonado utilizados por H. K. en el período comprendido entre el 1 de marzo de 2015 y el 19 de febrero de 2016.

¹⁰ El órgano jurisdiccional remitente aclara que, tras acumular esta pena a la pena de prisión de cuatro años y siete meses a la que H. K. había sido condenada por resolución del Viru Maakohus (Tribunal de Primera Instancia de Viru) de 22 de marzo de 2016, H. K. fue condenada a una penal global de cinco años y un mes de prisión.

¹¹ Se trata de un delito que consiste en influir en los tribunales. Debo señalar que el Viru Maakohus (Tribunal de Primera Instancia de Viru) modificó su calificación de los hechos imputados a este respecto a H. K. a tenor del artículo 323, apartado 1, del Código Penal, calificándolos de ataque a la libertad de los intervinientes en un proceso.

20. El 15 de marzo de 2016, la autoridad investigadora redactó un atestado relativo a los datos recabados de la empresa de telecomunicaciones sobre la base de dicha autorización en el que se especifican los días en que H. K. había llamado a los coacusados y había recibido llamadas de ellos y las fechas en que H. K. había remitido mensajes a los coacusados y los había recibido de estos. El Ministerio Fiscal quería probar ante el órgano jurisdiccional con dicho atestado, además de con otras pruebas, que desde la primavera de 2015 H. K. había amenazado telefónicamente a los coacusados en varias ocasiones.

21. El 20 de abril y el 6 de mayo de 2016, la autoridad investigadora volvió a redactar unos atestados en relación con los datos recabados de la empresa de telecomunicaciones en virtud de la misma autorización. En dichos atestados se indicaban las estaciones de base en cuyo ámbito de alcance se registraron los días 4, 27 y 31 de agosto de 2015, y del 1 al 3 de septiembre de 2015 llamadas telefónicas entrantes y salientes mediante los seis números de abonado utilizados por H. K. Con dichos atestados, además de con otras pruebas, el Ministerio Fiscal quería demostrarle al órgano jurisdiccional que fue H. K. quien había cometido los seis hurtos en las mencionadas fechas.

22. El 20 de abril de 2016, la autoridad investigadora redactó un atestado en el que se reproducían los datos relativos a dos números de abonado utilizados por H. K. Más concretamente, dicho atestado indica las estaciones base en cuyo ámbito de alcance, entre los días 16 y 19 de enero de 2015, se registraron llamadas telefónicas entrantes y salientes mediante dichos números de abonado. Con ese atestado, además de con otras pruebas, el Ministerio Fiscal quería probar que H. K. era la persona que entre los días 17 y 19 de enero de 2015 había retirado con la tarjeta bancaria de la víctima dinero en efectivo de un cajero automático.

23. Los datos en que se basaba el atestado fueron obtenidos de la empresa de telecomunicaciones en virtud de las autorizaciones conferidas los días de 28 de enero y 2 de febrero de 2015 en otro procedimiento penal por un fiscal de la Fiscalía de Distrito de Viru. Dicho procedimiento penal versaba sobre delitos tipificados con arreglo al artículo 200, apartado 2, números 7, 8 y 9, del Código Penal, a saber, dos robos con violencia cometidos los días 23 y 27 de enero de 2015 por un grupo armado utilizando la fuerza. Dichas autorizaciones permitieron a la autoridad investigadora exigir a la empresa de telecomunicaciones los datos a que se refiere el artículo 111¹, apartado 2, de la Ley de Comunicaciones Electrónicas relativos a los dos números de abonado y las distintas identidades internacionales del abonado móvil de H. K., en relación con el período comprendido entre el 1 de enero y el 2 de febrero de 2015.

24. De la descripción de los hechos del procedimiento principal que se ha hecho se desprende que el Ministerio Fiscal autorizó, con arreglo al artículo 90¹, apartado 2, de la Ley de Enjuiciamiento Criminal, a la autoridad investigadora para que dirigiera solicitudes de datos a la empresa de telecomunicaciones en el marco del procedimiento de instrucción. Se expidieron las autorizaciones relativas a los datos de los números de abonado de la acusada con el fin de investigar varios delitos, con una duración de un día, de aproximadamente un mes y de aproximadamente un año, respectivamente.

25. H. K. recurrió en apelación la resolución del Viru Maakohus (Tribunal de Primera Instancia de Viru) ante el Tartu Ringkonnakohus (Tribunal de Apelación de Tartu, Estonia), que desestimó dicho recurso mediante resolución del 17 de noviembre de 2017. H. K. interpuso entonces recurso de casación ante el Riigikohus (Tribunal Supremo) solicitando la anulación de las resoluciones dictadas en primera y segunda instancia, el archivo de las diligencias penales seguidas contra ella y su libre absolución.

26. H. K. alega que los atestados en los que se reproducen los datos obtenidos de la empresa de telecomunicaciones no son pruebas admisibles y que su condena basada en dichos atestados no está justificada. Considera que, con arreglo a la sentencia *Tele2 Sverige y Watson y otros*, las disposiciones del artículo 111¹ de la Ley de Comunicaciones Electrónicas que imponen a esos proveedores de servicios la obligación de conservar los datos relativos a las comunicaciones, así como el uso de estos datos para condenarla son contrarias al artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de los artículos 7, 8 y 11 y del artículo 52, apartado 1, de la Carta.

27. Según el tribunal remitente, se suscita de esta forma la cuestión de si los atestados controvertidos, redactados por la autoridad investigadora sobre la base de los datos contemplados en el artículo 111¹, apartado 2, de la Ley de Comunicaciones Electrónicas, exigidos a la empresa de telecomunicaciones en virtud de una autorización del Ministerio Fiscal, pueden considerarse pruebas admisibles.

28. El órgano jurisdiccional remitente puntualiza que los datos que los proveedores de servicios de comunicaciones electrónicas están obligados a conservar durante un período de un año incluyen, entre otros, el número de las líneas que efectúan y reciben la llamada, el nombre y la dirección del abonado, la fecha y la hora del inicio y de la finalización de la llamada, el servicio de telefonía fija o móvil utilizado, la identidad internacional del abonado móvil y la identidad internacional del equipo móvil de las líneas que efectúan y reciben la llamada, así como el identificador de celda al inicio de la llamada y los datos que permiten fijar la localización geográfica de la celda. Indica que se trata de datos vinculados a la transmisión de llamadas y mensajes por teléfono fijo o móvil, así como a la localización de los equipos terminales móviles, pero que no proporcionan ninguna indicación sobre el contenido de las comunicaciones.

29. Considera que, como se desprende de las sentencias *Tele2 Sverige y Watson y otros* y de 2 de octubre de 2018, *Ministerio Fiscal*,¹² la normativa de Derecho nacional que regule la conservación de los datos de tráfico y de localización y el acceso a esos datos en el marco de un procedimiento penal, como el artículo 111¹, apartados 2 y 4, de la Ley de Comunicaciones Electrónicas y el artículo 90¹, apartado 2, de la Ley de Enjuiciamiento Criminal, está comprendida en el ámbito de aplicación de la Directiva 2002/58.

30. Señala que la admisibilidad de las pruebas depende del cumplimiento de las normas de procedimiento relativas a la obtención de las pruebas. De ese modo, al evaluar la admisibilidad como medio probatorio de los atestados controvertidos en el procedimiento principal, también habrá de examinarse en qué medida era conforme al artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de los artículos 7, 8 y 11 y del artículo 52, apartado 1, de la Carta, recabar los datos de la empresa de telecomunicaciones en los que se basaron esos atestados.

31. A la vista de las sentencias *Tele2 Sverige y Watson y otros*¹³ y *Ministerio Fiscal*,¹⁴ el tribunal remitente se pregunta si debe interpretarse el artículo 15, apartado 1, de la Directiva 2002/58, a la luz de los artículos 7, 8 y 11 y del artículo 52, apartado 1, de la Carta, en el sentido de que el acceso de las autoridades nacionales a datos que permitan determinar el origen y el destino, la fecha, la hora y la duración, el tipo de servicio de comunicaciones, el equipo terminal utilizado y la localización de la utilización de equipos terminales móviles en relación con una comunicación por teléfono fijo o móvil de un investigado representa una injerencia tan grave en los derechos fundamentales consagrados en esos artículos de la Carta que dicho acceso debe limitarse a la lucha contra la delincuencia grave, con independencia del período para el que esas autoridades nacionales hayan solicitado acceder a los datos conservados.

¹² C-207/16, en lo sucesivo, «sentencia Ministerio Fiscal», EU:C:2018:788.

¹³ Punto 2 del fallo de dicha sentencia.

¹⁴ Apartados 53 y 57 de dicha sentencia.

32. A este respecto, el órgano jurisdiccional remitente considera que el período de tiempo para el que se exigen los datos de que se trata es un elemento esencial a la hora de evaluar la gravedad de la injerencia en los derechos fundamentales que podría constituir el acceso a los datos en cuestión. Cabe, pues, que tal injerencia no deba considerarse grave, cuando los datos solicitados versen únicamente sobre un breve período de tiempo, como, por ejemplo, un día. Considera que, en tal caso, por lo general, no es posible extraer, a partir de esos datos, conclusiones precisas acerca de la vida privada de la persona afectada, de modo que el acceso de las autoridades nacionales a dichos datos podría estar justificado por el objetivo de investigar y perseguir los delitos en general.

33. Además, el órgano jurisdiccional remitente se pregunta si el acceso a datos como los del procedimiento principal puede, a la vista de las enseñanzas que dimanar de la sentencia *Ministerio Fiscal*,¹⁵ estar justificado por ese mismo objetivo cuando la cantidad de datos a los que han tenido acceso las autoridades es reducida y la injerencia en los derechos fundamentales de que se trata no resulta, por lo tanto, grave. En cuanto a la cantidad de datos, considera fundamental tener en cuenta el tipo de datos (como los relativos al destinatario de la comunicación o la localización del equipo terminal) y su extensión temporal (por ejemplo, un día, mes o año). Según el órgano jurisdiccional remitente, cuanto más grave sea la infracción, mayor podrá ser la intensidad de la injerencia en los derechos fundamentales admitida en el procedimiento, lo que significa que será tanto mayor la cantidad de datos a los que las autoridades nacionales puedan acceder.

34. Por último, el tribunal remitente se pregunta si es posible considerar al Ministerio Fiscal una autoridad administrativa «independiente», en el sentido de la sentencia *Tele2 Sverige y Watson y otros*.¹⁶ Señala que, en Estonia, el Ministerio Fiscal es quien dirige el procedimiento de instrucción, cuyo objetivo es, especialmente, recoger pruebas. También subraya que la autoridad investigadora y el Ministerio Fiscal esclarecen las circunstancias de cargo y de descargo del investigado. Finalmente, apunta que las competencias del Ministerio Fiscal se ejercen en su nombre por un fiscal que cumplirá sus funciones de manera independiente, como resulta del artículo 30, apartados 1 y 2, de la Ley de Enjuiciamiento Criminal y de los artículos 1, apartados 1 y 1¹, y 2, apartado 2, de la Ley del Ministerio Fiscal.

35. En ese contexto, el órgano jurisdiccional remitente hace hincapié en que sus dudas sobre la independencia exigida por el Derecho de la Unión obedecen principalmente a que es el Ministerio Fiscal quien, una vez concluido el procedimiento de instrucción, formula la acusación contra la persona de que se trata si está convencido de que se han recabado todas las pruebas necesarias y procede. Dicho tribunal pone de relieve que, en tal caso, es el Ministerio Fiscal quien ejerce la acusación pública, por lo que también es parte en el procedimiento. El órgano jurisdiccional remitente también señala que el Tribunal Europeo de Derechos Humanos ya ha reconocido que, en determinadas circunstancias, pueden autorizarse medidas de vigilancia sin previo control judicial, a condición de que posteriormente se realice una revisión judicial.¹⁷

36. En estas circunstancias, el Riigikohus (Tribunal Supremo) decidió suspender el procedimiento y plantear al Tribunal de Justicia las siguientes cuestiones prejudiciales:

«1) ¿Debe interpretarse el artículo 15, apartado 1, de la Directiva [2002/58], a la luz de los artículos 7, 8, 11 y 52, apartado 1, de la [Carta], en el sentido de que, en el marco de un procedimiento penal, el acceso de las autoridades del Estado a los datos que permiten rastrear e identificar el origen y el destino de una comunicación por teléfono fijo o móvil de un investigado, determinar la fecha, la hora, la duración y la naturaleza de dicha comunicación, identificar el equipo de comunicación

¹⁵ Apartados 55 a 57 de dicha sentencia.

¹⁶ Apartado 120 y punto 2 del fallo de la citada sentencia.

¹⁷ El órgano jurisdiccional remitente cita, a este respecto, las sentencias del TEDH de 2 de septiembre de 2010, *Uzun c. Alemania* (CE:ECHR:2010:0902JUD003562305), §§ 71 a 74, y de 12 de enero de 2016, *Szabó y Vissy c. Hungría* (CE:ECHR:2016:0112JUD003713814), § 77.

utilizado y localizar el equipo de comunicación móvil utilizado representa una injerencia tan grave en los derechos fundamentales consagrados en los artículos antes mencionados de la Carta que dicho acceso, en el ámbito de la prevención, la investigación, el descubrimiento y la persecución de delitos, debe limitarse a la lucha contra la delincuencia grave, con independencia del período a que se refieran los datos conservados a los que tengan acceso las autoridades del Estado?

- 2) ¿Debe interpretarse el artículo 15, apartado 1, de la Directiva [2002/58], partiendo del principio de proporcionalidad recogido en la sentencia [Ministerio Fiscal], apartados 55 a 57, en el sentido de que, si la cantidad de datos a los que tienen acceso las autoridades del Estado a los que se hace referencia en la primera cuestión prejudicial no es grande (ni por la naturaleza de los datos ni por su extensión temporal), la injerencia que ello implica en los derechos fundamentales puede estar justificada en general por el objetivo de la prevención, la investigación, el descubrimiento y la persecución de delitos y de que los delitos contra los que se pretenda luchar mediante la injerencia deberán ser de mayor gravedad cuanto mayor sea la cantidad de datos a los que tengan acceso las autoridades del Estado?
- 3) ¿Significa el requisito mencionado en la sentencia [Tele2 Sverige y Watson y otros], punto 2 del fallo, de que el acceso de las autoridades competentes del Estado a los datos deba estar supeditado a un control previo por un órgano jurisdiccional o una autoridad administrativa independiente que el artículo 15, apartado 1, de la Directiva [2002/58] deba interpretarse en el sentido de que el Ministerio Fiscal, que dirige el procedimiento de instrucción, que al hacerlo está obligado por ley a actuar con independencia y solo está sometido a la ley, y que en el procedimiento de instrucción esclarece tanto las circunstancias de cargo como las de descargo del acusado, pero que posteriormente ejerce la acusación pública en el procedimiento judicial, puede tener la consideración de autoridad administrativa independiente?»

IV. Análisis

37. Mediante las cuestiones prejudiciales primera y segunda, el tribunal remitente desea fundamentalmente dilucidar si el artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de los artículos 7, 8 y 11 y del artículo 52, apartado 1, de la Carta, debe entenderse en el sentido de que entre los criterios de apreciación de la gravedad de la injerencia en los derechos fundamentales que representa el acceso por parte de las autoridades nacionales competentes a datos personales que los proveedores de servicios de comunicaciones electrónicas están obligados a conservar con arreglo a una normativa nacional se incluyen las categorías de los datos en cuestión y la duración del período para el que se solicita el acceso.

38. Antes de dar respuesta a esta cuestión prejudicial, deseo formular dos series de observaciones preliminares con objeto de poder contestar, por un lado, a los argumentos esgrimidos por algunos Estados miembros en relación con el ámbito de aplicación de la Directiva 2002/58 y, por otro, a la sugerencia formulada por la Comisión Europea de que se examine, en el marco del presente procedimiento prejudicial, la compatibilidad con el Derecho de la Unión de la normativa estonia, en tanto en cuanto impone a los proveedores de servicios de comunicaciones electrónicas la obligación de conservar varias categorías de datos personales generados en dichos servicios.

A. Observaciones preliminares

1. Sobre el ámbito de aplicación de la Directiva 2002/58

39. Los Gobiernos irlandés, húngaro y polaco plantean interrogantes en relación con el ámbito de aplicación de la Directiva 2002/58.

40. El Gobierno irlandés parece considerar que una normativa nacional relativa al acceso de las autoridades competentes en materia penal a datos conservados queda excluida, en virtud del artículo 1, apartado 3, de la Directiva 2002/58, del ámbito de aplicación de dicha Directiva.

41. Esta alegación debe descartarse con arreglo a la jurisprudencia del Tribunal de Justicia resultante de las sentencias *Tele2 Sverige* y *Watson y otros* y *Ministerio Fiscal*.

42. A este respecto, debe señalarse que el Tribunal de Justicia ha considerado que las medidas legales contempladas en el artículo 15, apartado 1, de la Directiva 2002/58 «están incluidas en el ámbito de aplicación de la Directiva, aun si se refieren a actividades propias de los Estados o [de] las autoridades estatales, ajenas a los ámbitos de actividad de los particulares, e incluso si las finalidades a las que deben responder tales medidas coinciden en esencia con las finalidades que persiguen las actividades mencionadas en el artículo 1, apartado 3, de la Directiva 2002/58». ¹⁸ En efecto, según el Tribunal de Justicia, «el artículo 15, apartado 1, de esa Directiva presupone necesariamente que las medidas nacionales que se establecen en ella están incluidas en el ámbito de aplicación de la citada Directiva, ya que esta solo autoriza expresamente a los Estados miembros a adoptarlas cumpliendo los requisitos que establece. Por otro lado, las medidas legales a que se refiere el artículo 15, apartado 1, de la Directiva 2002/58 regulan, a los efectos mencionados en dicha disposición, la actividad de los proveedores de servicios de comunicaciones electrónicas». ¹⁹

43. El Tribunal de Justicia concluyó de ello que «el mencionado artículo 15, apartado 1, de la Directiva 2002/58, en relación con su artículo 3, debe interpretarse en el sentido de que están incluidas en el ámbito de aplicación de dicha Directiva no solo una medida legislativa que obliga a los proveedores de servicios de comunicaciones electrónicas a conservar los datos de tráfico y los datos de localización, sino también una medida legislativa relativa al acceso de las autoridades nacionales a los datos conservados por dichos proveedores». ²⁰

44. En efecto, según el Tribunal de Justicia, «la protección de la confidencialidad de las comunicaciones electrónicas y de sus datos de tráfico, garantizada en el artículo 5, apartado 1, de la Directiva 2002/58, se aplica a las medidas adoptadas por todas las personas distintas de los usuarios, ya sean personas físicas o entidades privadas o públicas. Como confirma el considerando 21 de dicha Directiva, esta tiene como objetivo evitar “[todo] acceso” no autorizado a las comunicaciones, incluido “todo dato relativo a esas comunicaciones”, para proteger la confidencialidad de las comunicaciones electrónicas». ²¹

45. El Tribunal de Justicia añadió a esta argumentación que «las medidas legales que obligan a los proveedores de servicios de comunicaciones electrónicas a conservar datos personales o conceder a las autoridades nacionales competentes el acceso a estos datos implican necesariamente un tratamiento de dichos datos por esos proveedores [...]. Por tanto, tales medidas, en [cuanto] regulan las actividades de dichos proveedores, no pueden asimilarse a actividades propias de los Estados, mencionadas en el artículo 1, apartado 3, de la Directiva 2002/58». ²²

46. Como declaró el Tribunal de Justicia en su sentencia *Ministerio Fiscal*, ²³ de todos estos argumentos debe deducirse que la solicitud de acceso a datos personales conservados por proveedores de servicios de comunicaciones electrónicas, formulada en un procedimiento de instrucción penal, entra en el ámbito de aplicación de la Directiva 2002/58.

18 Sentencia *Ministerio Fiscal* (apartado 34 y jurisprudencia citada).

19 *Idem*.

20 Sentencia *Ministerio Fiscal* (apartado 35 y jurisprudencia citada).

21 Sentencia *Ministerio Fiscal* (apartado 36 y jurisprudencia citada).

22 Sentencia *Ministerio Fiscal* (apartado 37 y jurisprudencia citada).

23 Véase la sentencia *Ministerio Fiscal* (apartados 38 y 39).

47. Por otra parte, los Gobiernos húngaro y polaco argumentan que el Derecho de la Unión no regula la cuestión de la admisibilidad de las pruebas en los procedimientos penales.

48. Si bien es cierto que el Derecho de la Unión no se aplica, en el estado actual de su evolución, a las normas que regulan la admisibilidad de las pruebas en el proceso penal, el órgano jurisdiccional remitente ha puesto claramente de manifiesto que la interpretación del Derecho de la Unión que solicita le resulta necesaria para poder pronunciarse sobre la admisibilidad de las pruebas. En efecto, la admisibilidad de las pruebas depende de que se respeten los requisitos y normas procesales que regulan la obtención de esas pruebas. Por tanto, al apreciar la admisibilidad de los atestados controvertidos en el procedimiento principal como medio de prueba, el tribunal remitente debe examinar previamente la cuestión de en qué medida la obtención de los datos en que se basan tales atestados de la empresa de telecomunicaciones se ajustaba al artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de los artículos 7, 8 y 11 y del artículo 52, apartado 1, de la Carta. Pues bien, esta cuestión previa versa sobre un aspecto que, como he señalado anteriormente, se rige por el Derecho de la Unión. Así pues, en este aspecto, las normas nacionales aplicables en materia de práctica de la prueba deben respetar las exigencias derivadas de los derechos fundamentales garantizados por el Derecho de la Unión.²⁴ En estas circunstancias, considero que la alegación formulada por los Gobiernos húngaro y polaco no resulta pertinente.

2. Sobre la conservación de los datos de tráfico y de localización

49. Aunque las cuestiones prejudiciales planteadas por el órgano jurisdiccional remitente se refieren a los requisitos de acceso a los datos, la Comisión solicita al Tribunal de Justicia que también se pronuncie, en el marco del presente procedimiento prejudicial, sobre la problemática relativa a la conservación de los datos. A este respecto, señala fundamentalmente que, para que el acceso a los datos conservados sea legal, es preciso que la normativa nacional que obliga a los proveedores de servicios de comunicaciones electrónicas a conservar los datos generados en esos servicios responda a las exigencias del artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de la Carta, o que dichos proveedores hubiesen conservado, por su propia iniciativa, en particular, con fines comerciales, los datos en cuestión, ateniéndose a lo dispuesto en esa misma Directiva.

50. En relación con el procedimiento principal, la Comisión observa que los datos a los que ha tenido acceso la autoridad investigadora fueron conservados por los proveedores de servicios de comunicaciones electrónicas no por su propia iniciativa, con fines comerciales, sino en cumplimiento de la obligación de conservación que les impone el artículo 111¹ de la Ley de Comunicaciones Electrónicas. También señala que H. K. cuestiona la legalidad de las normas nacionales relativas tanto al acceso a los datos, como a su conservación.²⁵

51. Dicho esto, debo decir que, como ocurrió en la petición de decisión prejudicial que dio lugar a la sentencia Ministerio Fiscal,²⁶ las cuestiones prejudiciales formuladas por el órgano jurisdiccional remitente en el presente asunto no van dirigidas a que se establezca si los datos personales controvertidos en el procedimiento principal fueron conservados por los proveedores de servicios de comunicaciones electrónicas cumpliendo los requisitos establecidos en el artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de los artículos 7, 8 y 11 y del artículo 52, apartado 1, de la Carta. Las presentes cuestiones prejudiciales solo se refieren a la compatibilidad con estas

²⁴ Véase, en particular, por analogía, la sentencia de 10 de abril de 2003, Steffensen (C-276/01, EU:C:2003:228), apartado 71. En dicha sentencia, el Tribunal de Justicia también aborda esta problemática desde el punto de vista del principio de efectividad como límite a la autonomía procesal de los Estados miembros (apartados 66 a 68 de dicha sentencia).

²⁵ En este contexto, la Comisión subraya que el presente asunto se diferencia del que dio lugar a la sentencia Ministerio Fiscal.

²⁶ Véase la sentencia Ministerio Fiscal (apartados 49 y 50).

disposiciones de las condiciones que deben cumplirse para que pueda autorizarse, con arreglo a la normativa estonia, el acceso de las autoridades investigadoras nacionales a tales datos. Por este motivo, la discusión iniciada ante el Tribunal de Justicia se ha referido casi exclusivamente a esas condiciones de acceso.

52. En cualquier caso, el órgano jurisdiccional remitente puede basarse en la jurisprudencia sentada en la sentencia *Tele2 Sverige y Watson y otros* si considera necesario, a los efectos de dirimir el litigio principal, resolver acerca de la compatibilidad con el Derecho de la Unión del artículo 111¹ de la Ley de Comunicaciones Electrónicas.

53. En este aspecto, me limitaré a recordar que, según el Tribunal de Justicia, «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, debe interpretarse en el sentido de que se opone a una normativa nacional que establece, con la finalidad de luchar contra la delincuencia, la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica».²⁷

54. Incumbe al tribunal remitente comprobar, en su caso, si la normativa estonia impone a los proveedores de servicios de comunicaciones electrónicas una obligación de conservación de datos que revista ese carácter generalizado e indiferenciado, y extraer de ello las consecuencias a los efectos de la resolución del litigio principal. Si hubiera de considerarse que el régimen de conservación de datos establecido por la República de Estonia no es conforme con el Derecho de la Unión, por no ser proporcionado al objetivo que se persigue, tampoco cabría considerar que el acceso a los datos conservados de esta manera pueda justificarse al amparo de ese mismo objetivo.

55. Solo si esta obligación de conservación va acompañada de restricciones apropiadas, especialmente en relación con las categorías de datos a que se refiere y con la duración de la conservación, con arreglo a un régimen diferenciado en función del objetivo perseguido y estrictamente necesario para alcanzar tal objetivo, podrá superar la prueba de proporcionalidad.

56. No me detendré más, en las presentes conclusiones, en el concepto de «conservación limitada de los datos» que el Abogado General Sr. Campos Sánchez-Bordona examina pormenorizadamente en las conclusiones que presentó el 15 de enero de 2020 en el marco del asunto C-520/18, *Ordre des barreaux francophones et germanophone y otros*.²⁸

B. Sobre el acceso de las autoridades nacionales competentes a los datos conservados

1. Enseñanzas de la sentencia Tele2 Sverige y Watson y otros

57. El Tribunal de Justicia se enfrenta a la problemática relativa al acceso de las autoridades nacionales competentes a los datos conservados, «con independencia del alcance de la obligación de conservación de datos impuesta a los proveedores de servicios de comunicaciones electrónicas» y, en particular, con independencia del carácter generalizado o selectivo de una conservación de datos.²⁹ Esta apreciación guarda relación con el hecho de que el Tribunal de Justicia considera la conservación de datos y el acceso a estos como dos injerencias distintas en los derechos fundamentales protegidos por la Carta.

²⁷ Sentencia *Tele2 Sverige y Watson y otros* (apartado 112).

²⁸ EU:C:2020:7. Véanse, en particular, los puntos 72 a 107 de esas conclusiones.

²⁹ Véase la sentencia *Tele2 Sverige y Watson y otros* (apartado 113).

58. El acceso a los datos conservados «debe responder efectiva y estrictamente a uno de [los] objetivos» que figuran en el artículo 15, apartado 1, primera frase, de la Directiva 2002/58. También ha de existir una concordancia entre la gravedad de la injerencia y el objetivo perseguido. Si la injerencia se califica de «grave», solo puede justificarla la lucha contra la delincuencia grave.³⁰

59. Al igual que lo que prevalece en cuanto a la conservación de los datos, el acceso a los mismos por parte de las autoridades nacionales competentes solo puede autorizarse dentro de los límites de lo estrictamente necesario.³¹ Además, las medidas legales deben «establecer normas claras y precisas que indiquen en qué circunstancias y con arreglo a qué requisitos los proveedores de servicios de comunicaciones electrónicas deben conceder a las autoridades nacionales competentes acceso a los datos. Del mismo modo, una medida de esta naturaleza debe ser legalmente imperativa en Derecho interno».³² Más concretamente, las normativas nacionales deben «establecer [...] los requisitos materiales y procedimentales que regulen el acceso de las autoridades nacionales competentes a los datos conservados».³³

60. De lo anterior puede deducirse que «un acceso general a todos los datos conservados, con independencia de la existencia de una relación, por lo menos indirecta, con el fin perseguido, no puede considerarse limitado a lo estrictamente necesario».³⁴

61. Según el Tribunal de Justicia, «la normativa nacional de que se trate debe basarse en criterios objetivos para definir las circunstancias y los requisitos conforme a los cuales debe concederse a las autoridades nacionales competentes el acceso a los datos de los abonados o usuarios registrados. A este respecto, en principio solo podrá concederse un acceso en relación con el objetivo de la lucha contra la delincuencia a los datos de personas de las que se sospeche que planean, van a cometer o han cometido un delito grave o que puedan estar implicadas de un modo u otro en un delito grave».³⁵

62. En otros términos, el alcance de la normativa nacional que concede a las autoridades nacionales competentes el acceso a los datos conservados ha de estar suficientemente delimitado para impedir que ese acceso puede afectar a un número importante de personas, o incluso a todas las personas y a todos los medios de comunicación electrónica, así como al conjunto de datos conservados. En consecuencia, el Tribunal de Justicia ha invocado el criterio de la relación entre las personas afectadas y el objetivo perseguido.

63. Por otra parte, el Tribunal de Justicia ha establecido los requisitos que debe cumplir cualquier acceso de las autoridades nacionales competentes a los datos conservados.

64. En primer lugar, ese acceso debe estar «sujeto, en principio, salvo en casos de urgencia debidamente justificados, a un control previo de un órgano jurisdiccional o de una entidad administrativa independiente».³⁶ La decisión de este órgano jurisdiccional o de esta entidad debe producirse «a raíz de una solicitud motivada de esas autoridades, presentada, en particular, en el marco de procedimientos de prevención, descubrimiento o acciones penales».³⁷

30 Véase la sentencia *Tele2 Sverige y Watson y otros* (apartado 115).

31 Véase la sentencia *Tele2 Sverige y Watson y otros* (apartado 116).

32 Sentencia *Tele2 Sverige y Watson y otros* (apartado 117).

33 Sentencia *Tele2 Sverige y Watson y otros* (apartado 118).

34 Sentencia *Tele2 Sverige y Watson y otros* (apartado 119).

35 *Idem*.

36 Sentencia *Tele2 Sverige y Watson y otros* (apartado 120).

37 *Idem*.

65. Además, según el Tribunal de Justicia, es necesario que «las autoridades nacionales competentes a las que se conceda el acceso a los datos conservados informen de ello a las personas afectadas, en el marco de los procedimientos nacionales aplicables, siempre que esa comunicación no pueda comprometer las investigaciones que llevan a cabo esas autoridades».³⁸

66. Por último, los Estados miembros deben adoptar normas relativas a la seguridad y a la protección de los datos conservados por los proveedores de servicios de comunicaciones electrónicas para evitar los abusos y todo acceso ilícito a los datos.³⁹

2. Enseñanzas de la sentencia Ministerio Fiscal

67. En ese asunto, se planteó al Tribunal de Justicia la cuestión de la compatibilidad con el artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de los artículos 7 y 8 de la Carta, de una normativa nacional que contemplaba el acceso de las autoridades nacionales competentes, como la Policía Judicial, a datos personales o de filiación de los titulares de algunas tarjetas SIM.

68. En su sentencia, el Tribunal de Justicia señaló, por lo que se refiere al objetivo de la prevención, investigación, descubrimiento y persecución de delitos, que el tenor del artículo 15, apartado 1, primera frase, de la Directiva 2002/58 no limita este objetivo a la lucha contra los delitos graves, sino que se refiere a los «delitos» en general.⁴⁰

69. El razonamiento desarrollado por el Tribunal de Justicia deja claro el hecho de que debe haber, en relación con el acceso a los datos de las autoridades nacionales competentes, una correspondencia entre la gravedad de la injerencia y la gravedad de los delitos de que se trate.

70. Así, el Tribunal de Justicia recuerda, remitiéndose al apartado 99 de su sentencia *Tele2 Sverige y Watson y otros*, que ciertamente declaró que, «en materia de prevención, investigación, descubrimiento y persecución de delitos, solo la lucha contra la delincuencia grave puede justificar un acceso a datos personales conservados por los proveedores de servicios de comunicaciones electrónicas que, considerados en su conjunto, permiten extraer conclusiones precisas sobre la vida privada de las personas cuyos datos han sido conservados».⁴¹

71. No obstante, el Tribunal de Justicia precisa que «motiv[ó] esa interpretación basándose en que el objetivo perseguido por una norma que regula este acceso debe guardar relación con la gravedad de la injerencia en los derechos fundamentales en cuestión que supone la operación».⁴²

72. En efecto, «conforme al principio de proporcionalidad, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos solo puede justificar una injerencia grave el objetivo de luchar contra la delincuencia que a su vez esté también calificada de “grave”».⁴³

73. En cambio, «cuando la injerencia que implica dicho acceso no es grave, puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir “delitos” en general».⁴⁴

38 Sentencia *Tele2 Sverige y Watson y otros* (apartado 121).

39 Véase la sentencia *Tele2 Sverige y Watson y otros* (apartado 122).

40 Véase la sentencia *Ministerio Fiscal* (apartado 53).

41 Sentencia *Ministerio Fiscal* (apartado 54).

42 Sentencia *Ministerio Fiscal* (apartado 55).

43 Sentencia *Ministerio Fiscal* (apartado 56).

44 Sentencia *Ministerio Fiscal* (apartado 57).

74. En consecuencia, dichas consideraciones demandaban una apreciación acerca de si, a la vista de las circunstancias del caso de autos, la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta que habría supuesto el acceso de la Policía Judicial a los datos controvertidos en el litigio principal debía o no considerarse «grave».

75. Pues bien, a diferencia de lo que ocurría en su sentencia *Tele2 Sverige y Watson y otros*, el Tribunal de Justicia no calificó de «grave» la injerencia en los derechos protegidos en los artículos 7 y 8 de la Carta, que consistió en el acceso a los datos de que se trata.⁴⁵ En efecto, la solicitud de acceso tenía «por único objeto identificar a los titulares de las tarjetas SIM activadas durante un período de doce días con el número [de identidad internacional del equipo móvil] del teléfono móvil sustraído».⁴⁶ Se trataba del acceso únicamente «a los números de teléfono correspondientes a las tarjetas SIM, así como a los datos personales o de filiación de los titulares de dichas tarjetas, como su nombre, apellidos y, en su caso, la dirección. En cambio, esos datos no se [referían] [...] a las comunicaciones efectuadas con el teléfono móvil sustraído ni a la localización de este».⁴⁷

76. El Tribunal de Justicia dedujo de ello que «los datos a que se refiere la solicitud de acceso controvertida en el litigio principal solo permiten vincular, durante un período determinado, la tarjeta o tarjetas SIM activadas con el teléfono móvil sustraído y los datos personales o de filiación de los titulares de estas tarjetas SIM. Sin un cotejo con los datos relativos a las comunicaciones realizadas con esas tarjetas SIM y de localización, estos datos no permiten conocer la fecha, la hora, la duración o los destinatarios de las comunicaciones efectuadas con las tarjetas SIM en cuestión, ni los lugares en que estas comunicaciones tuvieron lugar, ni la frecuencia de estas con determinadas personas durante un período concreto. Por tanto, dichos datos no permiten extraer conclusiones precisas sobre la vida privada de las personas cuyos datos se ven afectados».⁴⁸

77. Una vez descartada la calificación de «injerencia grave», el Tribunal de Justicia pudo considerar que cabía invocar el objetivo de prevenir, investigar, descubrir y perseguir delitos en general, incluso los delitos no graves, para justificar la injerencia en cuestión.⁴⁹

78. El órgano jurisdiccional remitente plantea las cuestiones prejudiciales primera y segunda a la vista de esta jurisprudencia, con objeto de apreciar la gravedad de la injerencia que supone acceder a los datos en el proceso penal del litigio principal. Más precisamente, desea averiguar si las categorías de datos de que se trata y la duración del período para el que se solicita el acceso a esos datos son, desde esta perspectiva, criterios pertinentes.

3. Sobre los criterios que permiten evaluar la gravedad de la injerencia

79. Como se desprende de la jurisprudencia del Tribunal de Justicia, cuanto más numerosas sean las categorías de datos para los que se solicita acceso, más puede calificarse de «grave» la injerencia.

80. Dicho esto, las cuestiones prejudiciales primera y segunda planteadas por el órgano jurisdiccional remitente llevarán al Tribunal de Justicia a precisar si, además de las categorías de datos de que se trata, la extensión del período a que se refiere ese acceso también influye a la hora de determinar la gravedad de la injerencia.

⁴⁵ Sentencia Ministerio Fiscal (apartado 61).

⁴⁶ Sentencia Ministerio Fiscal (apartado 59).

⁴⁷ *Idem*.

⁴⁸ Sentencia Ministerio Fiscal (apartado 60).

⁴⁹ Sentencia Ministerio Fiscal (apartado 62).

81. En mi opinión, la respuesta debería ser afirmativa. Debo señalar, precisamente, que, en su sentencia *Ministerio Fiscal*, el Tribunal de Justicia también tuvo en cuenta, en su apreciación, la duración del período a que se refería el acceso, a saber, concretamente doce días.⁵⁰

82. Lo que permite apreciar la gravedad de la injerencia es la conjunción entre la naturaleza de los datos en cuestión y la duración del período al que se refiere el acceso. En efecto, ambos aspectos permiten comprobar si se respeta el criterio que determina la gravedad de la injerencia, es decir, si el acceso a los datos de que se trata puede permitir a las autoridades nacionales competentes extraer conclusiones precisas en relación con la vida privada de las personas cuyos datos se ven afectados por dicho acceso. Pues bien, para poder esbozar el retrato preciso de una persona, no solo es preciso que se acceda a varias categorías de datos, como los datos de identificación, de tráfico y los datos de localización, sino también que se acceda a los datos de un período suficientemente largo para poder revelar con suficiente precisión los rasgos principales de la vida de una persona.

83. En consecuencia, al igual que el número de categorías de datos afectadas, la duración del período para el que se solicitaban los datos a tenor de una autorización de acceso constituye un elemento esencial a los efectos de apreciar la gravedad de la injerencia en los derechos fundamentales de las personas afectadas. Como señala la Comisión, la acumulación de varias solicitudes de acceso referidas a una única persona también debe tenerse en cuenta, aunque tales solicitudes se refieran a períodos breves.

84. De la petición de decisión prejudicial se deduce que los datos a los que tuvo acceso la autoridad investigadora son los contemplados en el artículo 111¹, apartado 2, de la Ley de Comunicaciones Electrónicas. Estos datos permiten determinar el origen y el destino, la fecha, la hora y la duración, el tipo de servicio de comunicaciones, el equipo terminal utilizado y la localización de la utilización de equipos terminales móviles de una persona. Estos datos fueron transmitidos a la autoridad investigadora en relación con períodos de un día, de un mes y, prácticamente, de un año.

85. La apreciación del grado de injerencia en los derechos fundamentales que supone el acceso de las autoridades nacionales competentes a los datos personales conservados es el resultado de un examen concreto de las circunstancias propias de cada caso. En cada supuesto, incumbe al órgano jurisdiccional remitente apreciar si los datos para los que se autorizó el acceso podían permitir, en función de su naturaleza y de la duración del período al que se refería dicho acceso, llegar a conclusiones precisas sobre la vida privada de las personas afectadas.

86. Si tal fuera el caso, la injerencia debería calificarse de «grave», en el sentido de la jurisprudencia del Tribunal de Justicia y, por lo tanto, solo podría estar justificada en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos por un objetivo de luchar contra la delincuencia que haya que calificar a su vez también de «grave».⁵¹

4. Sobre la concordancia entre la gravedad de la injerencia y el objetivo perseguido

87. Según la jurisprudencia del Tribunal de Justicia, una injerencia en los derechos fundamentales calificada de «grave» requiere una justificación reforzada.

⁵⁰ Véase la sentencia *Ministerio Fiscal* (apartado 59). Véanse, en el mismo sentido, las conclusiones presentadas por el Abogado General Saugmandsgaard Øe en el asunto *Ministerio Fiscal* (C-207/16, EU:C:2018:300), quien señala que la solicitud de la Policía Judicial se refería a «un período claramente definido y reducido en el tiempo, a saber, doce días» (punto 33 y punto 84).

⁵¹ Sentencia *Ministerio Fiscal* (apartado 56).

88. Por lo que atañe a la gravedad de los presuntos delitos en relación con los cuales se ha concedido el acceso a los datos, la Comisión señala que la normativa nacional de que se trata en el procedimiento principal autoriza el acceso a los mismos, entre otras razones, para luchar contra los delitos en general.⁵²

89. Incumbe al tribunal remitente comprobar, en función de las circunstancias del caso de autos, si el acceso a datos como los del asunto principal responde efectiva y estrictamente a uno de los objetivos contemplados en el artículo 15, apartado 1, de la Directiva 2002/58. Es preciso recordar a este respecto que esa disposición no limita el objetivo de prevención, investigación, descubrimiento y persecución de delitos a la lucha contra los delitos graves, sino que se refiere a los «delitos» en general.⁵³

90. Si el órgano jurisdiccional remitente llega a la conclusión de que la injerencia debe calificarse de «grave», le corresponderá apreciar si la infracción en cuestión también puede calificarse de «grave» según el Derecho penal nacional.

91. A este respecto, estimo que debe dejarse a la apreciación de los Estados miembros la definición de lo que puede calificarse como «delito grave».

92. En efecto, y dependiendo de los sistemas jurídicos nacionales, una misma infracción puede castigarse con mayor o menor severidad. La definición de las circunstancias agravantes también puede variar en función de los Estados miembros.

93. Como, con razón, señala el Gobierno estonio, la sanción aplicable no constituye el único criterio para determinar la gravedad de las infracciones. También es preciso tener en cuenta la naturaleza de las infracciones, el daño que causan a la sociedad, el menoscabo que provocan en los intereses jurídicos y los efectos generales que producen en el ordenamiento jurídico nacional, así como en los valores de una sociedad democrática. El contexto histórico, económico y social específico de cada Estado miembro también tiene relevancia a estos efectos. Por otra parte, en relación con las circunstancias agravantes, procede preguntarse, por ejemplo, si los delitos han sido cometidos, bien de manera reiterada, bien contra colectivos vulnerables.

94. Para evaluar la proporcionalidad del acceso, también ha de tenerse en cuenta que, con arreglo al artículo 90¹, apartado 3, de la Ley de Enjuiciamiento Criminal, «los datos solamente podrán ser solicitados si ello resulta indispensable para alcanzar el objetivo del procedimiento penal». Como señala el Gobierno estonio, el criterio de la absoluta necesidad⁵⁴ obliga tanto a los investigadores como a las personas encargadas de conceder la autorización a considerar y apreciar qué datos son necesarios para la correcta tramitación del proceso penal, sin los cuales no sería posible, en un determinado asunto, indagar la verdad o detener a un presunto delincuente o criminal.

95. Añadiré que, como ha subrayado con razón el Gobierno francés, no siempre puede determinarse con precisión el grado de gravedad de una infracción ni su exacta calificación cuando se autoriza el acceso a datos conservados en una fase inicial de la investigación, de forma que podría resultar prematuro en esa fase subsumir esa infracción en la categoría de los delitos graves o en la de los delitos en general. El órgano jurisdiccional remitente deberá tomar en consideración esta incertidumbre, inherente a las investigaciones penales, cuyo objeto mismo consiste en contribuir a que se ponga de manifiesto la verdad, a la hora de valorar si el acceso reviste un carácter proporcionado.

⁵² Artículo 111¹, apartado 11, de la Ley de Comunicaciones Electrónicas y artículo 90¹ de la Ley de Enjuiciamiento Criminal.

⁵³ Véase la sentencia Ministerio Fiscal (apartado 53).

⁵⁴ También denominado «principio de la *ultima ratio*».

96. Dicho esto, la incertidumbre que puede haber al comienzo de la investigación penal sobre estos aspectos no puede eliminar la exigencia de que cada solicitud de acceso esté motivada por la necesidad de buscar pruebas relativas a un comportamiento delictivo o criminal concreto, sobre la base de una sospecha sustentada en pruebas objetivas. De esta manera, la finalidad de una solicitud de acceso no puede ser examinar, en un determinado período, todos los hechos y gestos de una persona, con la finalidad de buscar posibles infracciones. Por otra parte, si durante la investigación salen a la luz hechos nuevos, el acceso a los datos que los acrediten habrá de ser objeto de una nueva autorización de acceso.

97. Habida cuenta de las apreciaciones anteriores, sugiero al Tribunal de Justicia que declare que el artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de los artículos 7, 8 y 11 y del artículo 52, apartado 1, de la Carta, debe entenderse en el sentido de que entre los criterios de evaluación de la gravedad de la injerencia en los derechos fundamentales que representa el acceso por parte de las autoridades nacionales competentes a datos personales que los proveedores de servicios de comunicaciones electrónicas están obligados a conservar con arreglo a la normativa nacional se incluyen las categorías de datos en cuestión y la duración del período para el que se solicita dicho acceso. Incumbe al tribunal remitente apreciar, en función de la gravedad de la injerencia, si dicho acceso era estrictamente necesario para alcanzar el objetivo de garantizar la prevención, investigación, descubrimiento y persecución de delitos.

C. Control previo por un órgano jurisdiccional o una autoridad administrativa independiente

98. Para garantizar que el acceso de las autoridades nacionales competentes a los datos conservados se limite a lo estrictamente necesario para alcanzar el objetivo perseguido, el Tribunal de Justicia ha considerado fundamental que tal acceso «esté sujeto, en principio, salvo en casos de urgencia debidamente justificados, a un control previo *de un órgano jurisdiccional o de una entidad administrativa independiente*, y que la decisión de este órgano jurisdiccional o de esta entidad se produzca a raíz de una solicitud motivada de esas autoridades, presentada, en particular, en el marco de procedimientos de prevención, descubrimiento o acciones penales».⁵⁵

99. Mediante su tercera cuestión prejudicial, el tribunal remitente insta al Tribunal de Justicia a que precise los criterios que debe cumplir una autoridad administrativa para que pueda ser considerada «independiente», en el sentido de la sentencia *Tele2 Sverige y Watson y otros*. Más precisamente, el órgano jurisdiccional remitente se pregunta si es posible considerar al Ministerio Fiscal como una autoridad administrativa independiente, habida cuenta de que dirige el procedimiento de instrucción y ejerce la acusación pública.

100. Para dar respuesta a esta pregunta, considero útil tener en cuenta dos aspectos de la jurisprudencia del Tribunal de Justicia: por una parte, la jurisprudencia relativa a la independencia de las autoridades nacionales de control de la protección de los datos personales y, por otra parte, la jurisprudencia relativa a la independencia de la autoridad judicial emisora en el marco de la orden de detención europea.

101. Según el Tribunal de Justicia, la independencia es una característica esencial, afirmada, en particular, en el artículo 8, apartado 3, de la Carta, de las autoridades encargadas de controlar el respeto de las normas de la Unión en materia de protección de las personas físicas frente al tratamiento de datos personales para asegurar un control eficaz y fiable y reforzar la protección de las personas afectadas por las decisiones de dichas autoridades.⁵⁶

⁵⁵ Sentencia *Tele2 Sverige y Watson y otros* (apartado 120 y jurisprudencia citada), el subrayado es mío. Véase, en el mismo sentido, el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017 (EU:C:2017:592), apartados 202 y 208.

⁵⁶ Véase, en particular, la sentencia de 6 de octubre de 2015, *Schrems* (C-362/14, EU:C:2015:650), apartados 40 y 41 y jurisprudencia citada. Véase asimismo el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017 (EU:C:2017:592), apartado 229.

102. El Tribunal de Justicia ya declaró, a propósito del artículo 28, apartado 1, párrafo segundo, de la Directiva 95/46, que «las autoridades de control competentes para vigilar el tratamiento de datos personales han de disfrutar de la independencia que les permita ejercer sus funciones sin influencia externa. Esta independencia en particular excluye toda orden o influencia externa con independencia de la forma que revista, directa o indirecta, que pudiera orientar sus decisiones y, en consecuencia, poner en peligro el cumplimiento de la tarea que corresponde a dichas autoridades de establecer un justo equilibrio entre la protección del derecho a la intimidad y la libre circulación de datos personales».⁵⁷

103. El Tribunal de Justicia también ha hecho hincapié en la exigencia de que, habida cuenta de su papel de guardianas del derecho a la intimidad, esas autoridades de control deben estar «por encima de toda sospecha de parcialidad».⁵⁸

104. En la medida en que la tercera cuestión prejudicial planteada por el tribunal remitente afecta al Ministerio Fiscal, resulta también pertinente tener en cuenta los criterios formulados por el Tribunal de Justicia en su jurisprudencia relativa a la independencia de la autoridad judicial emisora en el marco de la orden de detención europea. Así, según el Tribunal de Justicia, el control efectuado al adoptarse una orden de detención «debe realizarse con objetividad, tomando en consideración todos los elementos inculpativos y exculpativos, y de manera independiente, lo que presupone la existencia de normas estatutarias y organizativas que permitan excluir todo riesgo de que la adopción de la decisión de emitir tal orden de detención esté sujeta a instrucciones externas, en particular del poder ejecutivo».⁵⁹ No obstante, es necesario tener presente que la apreciación concreta en cada caso por el Tribunal de Justicia de si el Ministerio Fiscal cumple dichos criterios⁶⁰ se realiza en el contexto específico de la emisión de la orden de detención europea, por lo que no puede trasladarse automáticamente a otros ámbitos, como el relativo a la protección de datos personales.

105. Precisado esto, los dos aspectos de la jurisprudencia del Tribunal de Justicia confluyen y ponen de relieve, en cada uno de los ámbitos a que se refieren, que la autoridad nacional competente para verificar el respeto de las normas del Derecho de la Unión debe tener carácter independiente, lo cual abarca dos requisitos.⁶¹ De una parte, esa autoridad no debe estar sometida a instrucciones o a presiones exteriores que puedan influir en sus decisiones. De otra parte, en virtud de su estatuto y de las tareas que le son encomendadas, dicha autoridad debe cumplir la exigencia de objetividad en el control que lleva a cabo, es decir, que debe ofrecer garantías de imparcialidad. Más particularmente, la apreciación por parte de una autoridad administrativa de la proporcionalidad del acceso a los datos conservados requiere que esté en condiciones de ponderar adecuadamente los intereses relacionados con la eficacia de la investigación en el marco de la lucha contra la delincuencia y aquellos que tienen que ver con la protección de los datos personales de las personas afectadas por el acceso a los datos. En este último aspecto, la exigencia de imparcialidad resulta por ello inherente al concepto de «autoridad administrativa independiente» puesto de manifiesto por el Tribunal de Justicia en su sentencia *Tele2 Sverige y Watson y otros*.

⁵⁷ Sentencia de 8 de abril de 2014, Comisión/Hungría (C-288/12, EU:C:2014:237), apartado 51 y jurisprudencia citada.

⁵⁸ Sentencia de 8 de abril de 2014, Comisión/Hungría (C-288/12, EU:C:2014:237), apartado 53 y jurisprudencia citada.

⁵⁹ Véase la sentencia de 9 de octubre de 2019, NJ (Fiscalía de Viena) (C-489/19 PPU, EU:C:2019:849), apartado 38 y jurisprudencia citada.

⁶⁰ Véase, por último, la sentencia de 12 de diciembre de 2019, JR y YC (Fiscales de Lyon y de Tours) (C-566/19 PPU y C-629/19 PPU, EU:C:2019:1077), en la que el Tribunal de Justicia consideró, en particular, que los elementos que se le habían presentados bastaban para demostrar que, «en Francia, los fiscales disponen de la facultad de apreciar de manera independiente, en particular respecto del poder ejecutivo, la necesidad y proporcionalidad de emitir una orden de detención europea y ejercen esa facultad de forma objetiva, teniendo en cuenta todas las pruebas de cargo y de descargo» (apartado 55 de dicha sentencia).

⁶¹ Sobre los dos aspectos de la exigencia de independencia, véase, por analogía, a propósito de los órganos jurisdiccionales nacionales competentes para resolver cuestiones relacionadas con la interpretación y la aplicación del Derecho de la Unión, la sentencia de 5 de noviembre de 2019, Comisión/Polonia (Independencia de los tribunales ordinarios) (C-192/18, EU:C:2019:924), apartados 108 a 110 y jurisprudencia citada.

106. Debe comprobarse si el Ministerio Fiscal, habida cuenta de los distintos cometidos que le encomienda la legislación de Estonia, cumple este requisito de independencia, en sus dos dimensiones, cuando ha de controlar el carácter estrictamente necesario del acceso a los datos. De esta forma, el concepto de «independencia» que debe caracterizar a la autoridad administrativa encargada de ese control reviste una dimensión funcional, en el sentido de que ha de apreciarse con arreglo al objetivo específico de ese control si dicha autoridad puede actuar sin intervenciones ni presiones exteriores que puedan influir en sus decisiones, respetando la objetividad y con estricta aplicación de la norma jurídica. En suma, el concepto de «autoridad administrativa independiente», en el sentido de la sentencia *Tele2 Sverige y Watson y otros*, está destinado a garantizar la objetividad, la fiabilidad y la eficacia de ese control.

107. Eso implica examinar si la legislación estonia que establece el estatuto y las funciones del Ministerio Fiscal puede suscitar dudas legítimas en las personas afectadas en cuanto a la impermeabilidad de los fiscales frente a elementos exteriores y en cuanto a su neutralidad en relación con los intereses a que se enfrentan a la hora de garantizar el control previo de la proporcionalidad del acceso a los datos.

108. El Ministerio Fiscal desempeña un cometido esencial en el desarrollo del procedimiento penal puesto que dirige el procedimiento de instrucción y tiene competencia, en particular, para ejercer la acción penal contra una persona sospechosa de haber cometido un delito a fin de que sea llevada ante un tribunal. En esa medida, debe ser considerado autoridad que participa en la administración de la justicia penal.⁶²

109. Como expresó el Tribunal de Justicia en relación con la Procura della Repubblica (Fiscal de la República, Italia), según una fórmula que considero extrapolable al presente asunto, «la función [del fiscal] no es resolver con total independencia un litigio, sino someterlo, en su caso, al conocimiento del órgano jurisdiccional competente, como parte del proceso que ejercita la acción penal».⁶³

110. Aunque el Ministerio Fiscal presenta, por tanto, en su estatuto, en su organización y en sus funciones, rasgos propios que lo diferencian de un tribunal y justifican su calificación como «autoridad que participa en la administración de la justicia penal en los Estados miembros», no es menos cierto que, desde el punto de vista funcional, cuando el Derecho nacional establece que la autoridad que ejerce el control previo de la proporcionalidad del acceso exigido por la sentencia *Tele2 Sverige y Watson y otros* es el Ministerio Fiscal, este último tiene que mostrar, en este aspecto, un grado de independencia análogo al de un tribunal. En efecto, el ejercicio de esta función por parte de autoridad administrativa, y no por un tribunal, no debe afectar a la objetividad, fiabilidad y eficacia de ese control.

111. A este respecto, procede recordar que, con arreglo al artículo 90¹, apartado 2, de la Ley de Enjuiciamiento Criminal, la autoridad investigadora podrá, con la autorización del Ministerio Fiscal en el procedimiento de instrucción o del órgano jurisdiccional en el procedimiento judicial, solicitar a un proveedor de servicios de comunicaciones electrónicas los datos enumerados en el artículo 111¹, apartados 2 y 3, de la Ley de Comunicaciones Electrónicas.

⁶² Véase, en particular, la sentencia de 27 de mayo de 2019, PF (Fiscal General de Lituania) (C-509/18, EU:C:2019:457), apartados 39 y 40.

⁶³ Sentencia de 12 de diciembre de 1996, X (C-74/95 y C-129/95, EU:C:1996:491), apartado 19.

112. Por otra parte, de la legislación estonia se desprende que, en el proceso penal, el Ministerio Fiscal dirige el procedimiento de instrucción, cuyo objetivo es reunir pruebas y establecer las demás condiciones para la apertura del juicio oral. Además, la autoridad investigadora y el Ministerio Fiscal esclarecerán las circunstancias de cargo y de descargo del investigado o acusado durante el procedimiento de instrucción. Si el Ministerio Fiscal está convencido de que se han recabado todas las pruebas necesarias y procede, formula la acusación contra la persona investigada y, en ese caso, ejerce la acusación pública en el juicio oral.

113. El órgano jurisdiccional remitente también señala que, aunque en el procedimiento penal el Ministerio Fiscal debe recabar la autorización de un juez instructor para las medidas con mayor injerencia en los derechos fundamentales (por ejemplo, para la mayoría de las medidas de vigilancia y el ingreso en prisión), las competencias del Ministerio Fiscal también comprenden decidir la adopción de actuaciones procesales con una injerencia intensa en los derechos fundamentales.⁶⁴

114. Las dudas expresadas por el tribunal remitente para calificar al Ministerio Fiscal de «autoridad administrativa independiente» en el sentido de la sentencia *Tele2 Sverige y Watson* y otros obedecen principalmente al hecho de que, tras el procedimiento de instrucción, si el Ministerio Fiscal está convencido de que se han recabado todas las pruebas necesarias en el procedimiento penal y procede, le corresponde formular la acusación contra el investigado. En este caso, el Ministerio Fiscal es quien ejerce la acusación pública en el juicio oral y, con ello, también es parte en el procedimiento jurisdiccional. Por ello, debido principalmente a su condición de parte acusadora, el tribunal remitente pone en duda la calificación del Ministerio Fiscal como «autoridad administrativa independiente» en el sentido de la sentencia *Tele2 Sverige y Watson* y otros.

115. Así expresadas, las dudas manifestadas por el órgano jurisdiccional remitente afectan más especialmente a la imparcialidad del Ministerio Fiscal en el control de la proporcionalidad del acceso a los datos por parte de los servicios de investigación que le corresponde realizar antes de autorizar ese acceso.

116. Antes de abordar este aspecto relativo a la imparcialidad, debo señalar que el artículo 1, apartado 1¹, de la Ley del Ministerio Fiscal dispone que este último «cumple de manera independiente las tareas que le atribuya la ley». Además, en virtud del artículo 2, apartado 2, de esa misma ley, «el fiscal ejercerá sus funciones de manera independiente y actuará únicamente de conformidad con la ley y su conciencia».⁶⁵

117. A este respecto, el Gobierno estonio señala que, si bien el Ministerio Fiscal está incluido en el Ministerio de Justicia, la legislación estonia niega a este último toda posibilidad de formular apreciación alguna en relación con un procedimiento concreto y de intervenir en un procedimiento penal en curso. Aclara que la vulneración de la independencia del Ministerio Fiscal constituiría una infracción sancionable.

118. Como consecuencia de ello, aunque no cabe dudar de la independencia del Ministerio Fiscal en las funciones que tiene asignadas con arreglo a la legislación estonia, sí es legítimo, en mi opinión, albergar dudas acerca de la aptitud del Ministerio Fiscal para ejercer un control previo neutral y objetivo de la proporcionalidad del acceso a los datos cuando cabe la posibilidad de que recaiga en él, al mismo tiempo, en un determinado asunto, el ejercicio de funciones como la dirección de la investigación penal, la decisión de ejercer la acción penal y el ejercicio de la acusación pública en el juicio oral.

⁶⁴ Por ejemplo, es el Ministerio Fiscal quien autoriza la vigilancia encubierta de una persona, un bien o un lugar, así como, en muchos casos, el registro.

⁶⁵ Véase también, en el mismo sentido, el artículo 30, apartado 2, de la Ley de Enjuiciamiento Criminal.

119. Es cierto que varios elementos que figuran en la legislación estonia garantizan que el Ministerio Fiscal actúe en las funciones que asume respetando la exigencia de imparcialidad.

120. Por ejemplo, en virtud del artículo 211, apartado 2, de la Ley de Enjuiciamiento Criminal, el Ministerio Fiscal esclarecerá las circunstancias de cargo y de descargo del investigado o acusado.

121. Por otra parte, como resulta del artículo 1, apartado 1, de la Ley del Ministerio Fiscal, este último tiene la obligación de garantizar la legalidad del procedimiento de instrucción, cuya dirección tiene encomendada. Además, con arreglo a los artículos 1, apartado 1¹, y 2, apartado 2, de esa misma ley, el Ministerio Fiscal debe ejercer sus funciones observando la ley. Ello implica que, cuando dirige el procedimiento de instrucción, el objetivo del Ministerio Fiscal no solo debe ser garantizar su eficacia, sino también que ese procedimiento no se lleve a cabo con un menoscabo desproporcionado del derecho a la vida privada de las personas afectadas. En efecto, cabe considerar que la autorización de acceder a los datos conservados forma parte de un cometido más general del Ministerio Fiscal, que consiste en el control de la legalidad de los medios utilizados por los servicios de investigación, en particular, de la proporcionalidad de los actos de investigación a la vista de la naturaleza y gravedad de los hechos.

122. Por consiguiente, podría argüirse que, precisamente porque dirige el procedimiento de instrucción, el Ministerio Fiscal está en condiciones de evaluar si, a la vista de las características específicas de cada asunto, resulta estrictamente necesario acceder a datos conservados por los operadores del sector de telecomunicaciones —a falta de pruebas alternativas—, con objeto de hacer avanzar la investigación sobre un presunto delito.

123. No es menos cierto que, desde el punto de vista de las personas afectadas por la solicitud de acceso a los datos, la circunstancia de que la autoridad administrativa que debe comprobar si ese acceso es estrictamente necesario en el marco de la investigación sea al mismo tiempo la que puede promover actuaciones judiciales contra ellas y ejercer luego la acusación pública en un eventual juicio posterior puede, en mi opinión, debilitar las garantías de imparcialidad establecidas por la legislación estonia. Desde ese punto de vista, puede existir un potencial conflicto entre esas funciones del Ministerio Fiscal, por un lado, y la exigencia de neutralidad y de objetividad del control previo de la proporcionalidad del acceso a los datos, por otra parte.

124. En efecto, en el contexto de sus funciones, el Ministerio Fiscal debe recabar las pruebas, apreciar su pertinencia y extraer conclusiones respecto a la culpabilidad de la persona investigada. Corresponde a esa autoridad estatal presentar y fundamentar la acusación en el marco de la acción pública que ha de ejercer en el juicio oral, siendo en consecuencia parte en el procedimiento. Como consecuencia de sus funciones, el Ministerio Fiscal está sujeto a una exigencia probatoria que puede resultar, a los ojos de las personas investigadas como sospechosas de la comisión de un delito, incompatible con la aptitud de esa misma autoridad para llevar a cabo, de manera neutral y objetiva, un control previo de la proporcionalidad del acceso a los datos.

125. Como señala la Comisión, el riesgo podría residir en que las personas afectadas consideren que, debido a la acumulación de los cometidos que le corresponden, el Ministerio Fiscal tiene interés en que se dé un amplio acceso a sus datos, tanto si son de cargo como de descargo. Además, las personas sospechosas de haber cometido una infracción pueden albergar dudas legítimas sobre la imparcialidad del Ministerio Fiscal cuando autoriza el acceso a sus datos, dado que puede actuar contra ellas en un proceso posterior como parte acusadora. Pues bien, estimo que la exigencia de que la autoridad administrativa encargada de realizar el control previo sea imparcial, establecida en la sentencia *Tele2 Sverige y Watson y otros*, supone cierta distancia y neutralidad en relación con los intereses que pueden colisionar en el procedimiento de instrucción, a saber, por una parte, la eficacia de este último y, por otra parte, la protección de los datos personales de las personas afectadas. Según

la Comisión, la situación podría ser diferente si el Ministerio Fiscal estuviera organizado internamente de tal manera que el fiscal que tuviera que pronunciarse sobre la solicitud de acceso no desempeñara ninguna función en el procedimiento de instrucción ni en las etapas posteriores del procedimiento, incluida la acusación pública.

126. Dado que, como se confirmó en la vista, la fiscalía está organizada de manera jerárquica en la República de Estonia, no estoy seguro de que esta sugerencia de la Comisión pueda subsanar los inconvenientes generados por la acumulación de funciones atribuidas al Ministerio Fiscal por la legislación estonia. En cualquier caso, esto no desmerece la pertinencia de la idea que subyace en esa sugerencia, a saber, que el control previo de la proporcionalidad del acceso a los datos deba realizarse por una autoridad administrativa que, por una parte, no esté directamente implicada en la realización de la investigación penal de que se trata y, por otra parte, tenga una posición neutral frente a las partes del procedimiento penal. No podría reprocharse a esa autoridad, desvinculada de los intereses relacionados con la investigación y con la acusación pública en el procedimiento de que se trata, que priorice los intereses de la investigación a costa de los de protección de los datos relativos a las personas afectadas. En ese caso, dicha autoridad podría adoptar, con una imparcialidad absoluta, la decisión de limitar el acceso a los datos conservados a lo estrictamente necesario para alcanzar el objetivo perseguido, con arreglo a las exigencias del artículo 15, apartado 1, de la Directiva 2002/58, en la interpretación que recibe del Tribunal de Justicia en las sentencias de 8 de abril de 2014, *Digital Rights Ireland y otros*⁶⁶ y *Tele2 Sverige y Watson y otros*. Al mismo tiempo, soy consciente de que el establecimiento de una visión externa a los intereses relacionados con el procedimiento de que se trata no debe hacerse a costa de rebajar la eficacia de la investigación, persecución y represión de los delitos.

127. Con el fin de respetar la autonomía procesal de los Estados miembros, el Tribunal de Justicia no debería detenerse a analizar más a fondo la organización general de la administración de la justicia en los Estados miembros, como tampoco la de la organización interna de las fiscalías. Corresponde a los Estados miembros adoptar los instrumentos idóneos para garantizar que el control previo del acceso a los datos conservados garantice un justo equilibrio entre los intereses relacionados con la eficacia de la investigación penal y el derecho a la protección de los datos de las personas afectadas por ese acceso.

128. Debo finalizar aclarando que, en mi opinión, la falta de un control previo realizado por una autoridad administrativa «independiente» en el sentido de la sentencia *Tele2 Sverige y Watson y otros* no puede compensarse con la existencia de un control jurisdiccional que pueda realizarse una vez autorizado el acceso.⁶⁷ En caso contrario, la exigencia del carácter previo del control perdería su razón de ser, que consiste en impedir que se autorice un acceso desproporcionado a los datos conservados en relación con el objetivo de investigar, perseguir y reprimir los delitos.

129. A la vista de las apreciaciones anteriores, sugiero al Tribunal de Justicia que responda a la tercera cuestión prejudicial que el artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de los artículos 7, 8 y 11 y del artículo 52, apartado 1, de la Carta, debe interpretarse en el sentido de que la exigencia en virtud de la cual el acceso de las autoridades nacionales competentes a los datos conservados ha de someterse a un control previo de un órgano jurisdiccional o de una autoridad administrativa independiente no se cumple cuando la normativa nacional establece que ese control lo realice el Ministerio Público, al que se le encomienda la función de dirigir el procedimiento de instrucción, y que puede ejercer, al mismo tiempo, la acusación pública.

⁶⁶ C-293/12 y C-594/12, EU:C:2014:238.

⁶⁷ Según las pruebas presentadas al Tribunal de Justicia en la vista, en Derecho estonio, ese control jurisdiccional puede realizarse al final del procedimiento de instrucción, cuando un sospechoso al que se le comunicó el sumario decida impugnar un acto de ese procedimiento, o bien durante el juicio oral.

V. Conclusión

130. A la luz de lo que antecede, propongo al Tribunal de Justicia que responda a las cuestiones prejudiciales planteadas por el Riigikohus (Tribunal Supremo, Estonia) en los siguientes términos:

- «1) El artículo 15, apartado 1, de la 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), en su versión modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, interpretado a la luz de los artículos 7, 8 y 11, así como del artículo 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea, debe entenderse en el sentido de que entre los criterios de evaluación de la gravedad de la injerencia en los derechos fundamentales que representa el acceso por parte de las autoridades nacionales competentes a datos personales que los proveedores de servicios de comunicaciones electrónicas están obligados a conservar con arreglo a la normativa nacional se incluyen las categorías de datos en cuestión y la duración del período para el que se solicita dicho acceso. Incumbe al tribunal remitente apreciar, en función de la gravedad de la injerencia, si dicho acceso era estrictamente necesario para alcanzar el objetivo de garantizar la prevención, investigación, descubrimiento y persecución de delitos.
- 2) El artículo 15, apartado 1, de la Directiva 2002/58, en su versión modificada por la Directiva 2009/136, interpretado a la luz de los artículos 7, 8 y 11 y del artículo 52, apartado 1, de la Carta de los Derechos Fundamentales, debe interpretarse en el sentido de que la exigencia en virtud de la cual el acceso de las autoridades nacionales competentes a los datos conservados ha de someterse a un control previo de un órgano jurisdiccional o de una autoridad administrativa independiente no se cumple cuando la normativa nacional establece que ese control lo realice el Ministerio Público, al que se le encomienda la función de dirigir el procedimiento de instrucción, y que puede ejercer, al mismo tiempo, la acusación pública.»