IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

ARTÍCULO

La regulación sobre la conservación de datos en el sector de las comunicaciones electrónicas o telecomunicaciones: estado de la cuestión

Andoni Polo Roca
Abogado

Fecha de presentación: febrero de 2020
Fecha de aceptación: enero de 2021
Fecha de publicación: octubre de 2021

Resumen

La Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre conservación de datos estableció la obligación de los operadores de telecomunicaciones de conservación generalizada e indiferenciada de los datos relativos a las comunicaciones electrónicas (telefonía fija, móvil o internet) con fines de investigación, detección y enjuiciamiento de delitos graves. El TJUE, sin embargo, hizo tambalear las bases de dicha regulación con los casos *Digital Rights Ireland y Seitlinger y otros* (2014) y *Tele2 Sverige y Watson y otros* (2016), en los que declaró contraria al Derecho de la Unión la conservación de datos en los términos de la Directiva de 2006. Por su parte, en el Derecho español, fue la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones la que hizo la transposición de la Directiva de Conservación de Datos (2006), si bien, a la luz de la doctrina del TJUE, su aplicación podría ser cuestionada (al igual que las demás legislaciones nacionales que la traspusieron). No obstante, lejos de ser una cuestión pacífica, se han venido manteniendo posiciones muy distintas por parte del Tribunal Supremo en sus resoluciones o de la doctrina. A ello se le añaden, además, los pronunciamientos posteriores del TJUE, en especial el caso *La Quadrature du Net y otros contra Premier ministre y otros* (2020), en los que el TJUE ha ido sentando las bases de la conservación de datos en el ámbito de las comunicaciones electrónicas o telecomunicaciones.

© 2021, Andoni Polo Roca
© de esta edición: 2021, Universitat Oberta de Catalunya

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Palabras clave
conservación de datos, datos de tráfico, datos de localización, comunicaciones electrónicas, directiva sobre conservación de datos, TJUE

Tema
Derecho Administrativo, Derecho de las Telecomunicaciones, Derecho de la Unión Europea

The regulation on data retention in the electronic communications sector or the telecommunications sector: state of the matter

Abstract
Directive 2006/24/EC of the European Parliament and of the Council, of 15 March 2006, on data retention, established the obligation (to telecommunications operators) to retain electronic communications data (fixed network telephony, mobile telephony or Internet) for the purpose of the investigation, detection and prosecution of serious crime. The ECJ, however, destabilised the bases of said regulation with the case Digital Rights Ireland and Seitlinger and Others (2014), as well as with the case Tele2 Sverige and Watson and Others (2016), in which it declared that data retention in the terms of the 2006 Directive was contrary to EU law. With respect to Spanish law, it was Law 25/2007, of 18 October, on data retention relating to electronic communications and the public communications networks, which made the transposition of the Data Retention Directive (2006), but in the light of the ECJ doctrine, its application could be questioned (as well as the other national legislations that transposed it). However, far from being a harmonious matter, very different positions have been maintained by the Supreme Court of Spain in its decisions and in relation to the doctrine. Furthermore, to this may be added the subsequent pronouncements of the ECJ, particularly the case of La Quadrature du Net and Others versus Premier Ministre and Others (2020), in which the ECJ has laid the foundations for data retention in the field of electronic communications or telecommunications.

Keywords
data retention, traffic data, location data, electronic communications, data retention directive, ECJ

Topic
Administrative Law, Telecommunications Law, European Union Law

© 2021, Andoni Polo Roca
© de esta edición: 2021, Universitat Oberta de Catalunya

1. Introducción

La conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (telefonía fija, móvil o internet) supone un terreno bastante controvertido, dentro del Derecho de las Telecomunicaciones, que afecta directamente a la protección de datos y a la intimidad misma.

Así, con el almacenamiento y conservación (o retención) de los datos de comunicaciones electrónicas («metadatos»[1]) –incluso únicamente con la de las direcciones del remitente y del destinatario–, se puede reconstruir la trama de las relaciones personales y sociales, económicas, concernientes a la fe religiosa, etc.[2] Por lo que la vulneración comenzaría en la protección de datos y se extendería hacia otros derechos (intimidad, libertad ideológica, libertad religiosa, libertad sindical, etc.). La regulación, por ello, debe ser muy garantista y cuidadosa, y se debería tener siempre en cuenta el principio de minimización de datos (*data minimisation*)[3].

En el año 2006 la Unión Europea (UE) reguló este sector con la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre Conservación de Datos[4] (en lo sucesivo, DCD) que establecía la obligación de los operadores de telecomunicaciones de «conservación generalizada e indiferenciada» de todos los datos de comunicaciones electrónicas de todos los usuarios (y el acceso a ellos por parte de las autoridades competentes), y cuya transposición en España se hizo en virtud de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (en adelante, LCD).

El régimen que estableció la DCD –la conservación masiva generalizada e indiferenciada–, sin embargo, fue puesto en tela de juicio por la doctrina, que consideró que la Directiva convertía a todos los ciudadanos en potenciales sospechosos[5]; por ello se afirmó que no estaba en juego solamente la protección de datos, sino, también, la presunción de inocencia misma[6].

Se afirmó, asimismo, que el régimen de la DCD suponía una especie de control permanente de los usuarios de comunicaciones electrónicas[7]; incluso la vigilancia (vigilancia de datos, *dataveillance*) de la ciudadanía de la UE[8].

En este contexto, el Tribunal de Justicia de la Unión Europea (TJUE) se pronunció en el año 2014 anulando por completo la DCD de 2006, pero ello abrió una gran incógnita: en qué lugar quedaban las legislaciones nacionales de los Estados miembros que traspusieron la Directiva (en especial, la LCD), y, también, la conservación de datos misma. A todo ello, además, le han seguido de distintos pronunciamientos del Tribunal de Luxemburgo que han ido moldeando este ámbito.

1. Cuando hablamos de metadatos de comunicaciones electrónicas hacemos referencia a todos aquellos datos que «rodean» la comunicación electrónica, no a su contenido.
2. RODOTÀ, S. (2006). «La conservación de los datos de tráfico en las comunicaciones electrónicas». *IDP. Revista de Internet, Derecho y Política*, núm. 3, págs. 53-60, pág. 57.
3. TRACOL, X. (2017). «The judgment of the Grand Chamber dated 21 december 2016 in the two joint Tele2 Sverige and Watson cases: the need for a harmonised legal framework on the retention of data at EU level. *Computer Law & Security Review,* vol. 33, núm. 4, págs. 541-552, pág. 546.
4. Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.
5. RODOTÀ, S. (2006). «La conservación de los datos...», *op. cit*., pág. 57.
6. RODOTÀ, S. (2006). «La conservación de los datos...», *op. cit*., pág. 58.
7. *Cfr.* FERNÁNDEZ RODRIGUEZ, J. J. (2016). «Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente». *Revista española de derecho constitucional,* vol. 36, núm. 108, págs. 93-122.
8. MILAJ, J. (2015). «Invalidation of the data retention directive: extending the proportionality test». *Computer Law & Security Review*, vol. 31, núm. 5, págs. 604-617, pág. 611.

© 2021, Andoni Polo Roca
© de esta edición: 2021, Universitat Oberta de Catalunya

2. Marco normativo del análisis

2.1. La Directiva *e-Privacy* (2002) y su artículo 15.1

La norma básica en todo este análisis es la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, sobre la privacidad y las comunicaciones electrónicas[9] (en lo sucesivo, Directiva *e-Privacy*), en su versión modificada en 2009[10] –cabe mencionar que actualmente la Directiva está siendo objeto de reforma, con la Propuesta de Reglamento *e-Privacy*[11]–.

Tal como establece la Directiva *e-Privacy*, al hablar de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, hacemos referencia a los «datos de tráfico» y a los «datos de localización»: es decir, a cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma –art. 2, letra b)–, o a cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario –art. 2, letra c)–, respectivamente[12].

El TJUE ya declaró que los datos de comunicaciones electrónicas constituyen datos de carácter personal, ya que, según el Tribunal, considerados en su conjunto, «permiten extraer conclusiones muy precisas sobre la vida privada de las personas»[13].

Asimismo, en esta cuestión, debemos distinguir dos niveles distintos de injerencia en los derechos fundamentales: la conservación en sí y el consiguiente acceso a esos datos por las autoridades[14]. Por tanto, la conservación *per se* supone una injerencia en el derecho a la vida privada, siendo irrelevante que los datos tengan o no carácter de sensible[15]; y, además, el acceso de las autoridades públicas a los datos de telecomunicaciones supone una inmisión adicional[16].

Ello casa con la doctrina del Tribunal Europeo de Derechos Humanos (TEDH), que establece que la mera conservación de estos datos supone una injerencia *per se* en el derecho a la vida privada, independientemente de que se acceda (o no) a ellos más tarde y de la manera que se haga[17].

No obstante lo anterior, la Directiva *e-Privacy* recogió una habilitación especial en su artículo 15.1 que establece que los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en la Directiva (entre ellos, eliminación o anonimización de los datos de tráfico y localización), cuando tal limitación constituya «una medida necesaria

9. 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.
10. La Directiva *e-Privacy* de 2002 fue modificada por la siguiente norma: Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) núm. 2006/2004 sobre la cooperación en materia de protección de los consumidores.
11. Es voluntad de la UE actualizar la Directiva *e-Privacy* (2002), que será sucedida por el futuro Reglamento *e-Privacy* (aún propuesta); no obstante, su aprobación lleva años demorándose, con más de diez borradores de la norma a sus espaldas. *Cfr.* Propuesta de Reglamento, del Parlamento Europeo y del Consejo, sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas). COM/2017/010 final-2017/03 (COD).
12. Esto no fue modificado en la versión de 2009; salvo por un mínimo cambio en las letras de los apartados. *Cfr.* art. 2, apdo. 2.º, de la Directiva 2009/136/CE.
13. STJUE (Gran Sala), de 21 de diciembre de 2016, asuntos acumulados C-203/15 y C-698/15, *Tele2 Sverige y Watson y otros,* § 99; y STJUE (Gran Sala) de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12 *Digital Rights Ireland y Seitlinger y otros*, § 27.
14. RUCZ, M.; KLOOSTERBOER, S. (2020). «Data retention revisited booklet». *European Digital Rights (EDRi)*, pág. 9.
15. STJ, de 20 de mayo de 2003, asuntos acumulados C-465/00, C-138/01 y C-139/01, *Rechnungshof* (C-465/00) *contra Österreichischer Rundfunk y otros* y *Christa Neukomm* (C-138/01) y *Joseph Lauermann* (C-139/01) *contra Österreichischer Rundfunk*, § 75.
16. STEDH, de 4 de mayo de 2000, caso *Rotaru c. Rumanía*, asunto n.º 28341/95, ap. 46; y STEDH, de 29 de junio de 2006, caso *Weber y Saravia c. Alemania*, asunto n.º 54934/00, ap. 79.
17. STEDH, de 4 de diciembre de 2008, caso *S. y Marper c. Reino Unido*, asuntos n.º 30562/04 y n.º 30566/04, ap. 67.

© 2021, Andoni Polo Roca
© de esta edición: 2021, Universitat Oberta de Catalunya

proporcionada y apropiada en una sociedad democrática» para proteger la:

- «seguridad nacional»
- «defensa»
- «seguridad pública»
- «prevención, investigación, descubrimiento y persecución de delitos».

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 dichos motivos, teniendo estos carácter exhaustivo (*números clausus*).

Por tanto, el artículo 15 de la Directiva *e-Privacy* recoge una habilitación de conservación de datos de comunicaciones electrónicas por plazo limitado, motivos justificados y siendo siempre proporcional (ello se mantuvo intacto en las versiones de 2002 y 2009 de la Directiva[18]).

2.2. La Directiva sobre Conservación de Datos (2006)

En el año 2006, la UE aprobó la Directiva sobre Conservación de Datos (DCD) que establecía la obligación de los proveedores de servicios de comunicaciones electrónicas y explotadores de redes públicas de telecomunicaciones de conservar los datos de comunicaciones electrónicas con fines de investigación, detección y enjuiciamiento de delitos graves (art. 1.1); ello, asimismo, con el acceso de las autoridades nacionales competentes a los datos conservados (art. 4). Es decir: conservación y acceso (dos niveles de injerencia, como hemos mencionado).

La DCD fue la norma con la que la UE quiso armonizar las legislaciones que los Estados miembros pudieran elaborar con base en el mencionado artículo 15.1 de la Directiva *e-Privacy* en relación con la conservación de estos datos con fines de «prevención, investigación, descubrimiento y persecución de delitos» (en vez de dejar que cada Estado miembro elaborara su propia legislación nacional en esta materia). Así, la DCD modificó la Directiva *e-Privacy* y estableció que el artículo 15.1 no sería de aplicación a la conservación de datos de comunicaciones electrónicas con fines de «prevención, investigación, descubrimiento y persecución de delitos»[19] (art. 11 de la DCD), ya que en dicho ámbito se aplicaría la DCD (*lex specialis*).

Los datos que los operadores están obligados a conservar o retener *ex* DCD son los siguientes (art. 5 de la DCD): datos necesarios para rastrear e identificar el origen y destino de una comunicación (número de teléfono, IP, dirección del abonado, etc.), datos necesarios para identificar la fecha, hora y duración de una comunicación, datos necesarios para identificar el tipo de comunicación (voz, SMS, datos, MMS, etc.), datos necesarios para identificar el equipo de comunicación (IMEI, IMSI, DSL...) y datos necesarios para identificar la localización del equipo de comunicación móvil; en ningún caso podrán conservarse datos que revelen el contenido de la comunicación. Se conservan, por tanto, los «metadatos» de las comunicaciones electrónicas mantenidas por los usuarios de éstas: el continente, pero en ningún caso el contenido.

De este modo, la DCD estableció la obligación de «conservación generalizada e indiferenciada» (previa al posible delito) de todos los datos de comunicaciones electrónicas de todos los ciudadanos de la UE por parte de los operadores de telecomunicaciones (datos de telefonía de red fija, telefonía móvil, acceso a Internet, telefonía por Internet, correo electrónico, etc.).

Es por ello que se afirmó que esta convertía a todos los ciudadanos en potenciales sospechosos[20].

18. Salvo por la introducción del apartado 1 *ter*. en el artículo 15 (lo cual carece de relevancia a efectos de este análisis). *Cfr*. art. 2, apdo 9.º, de la Directiva 2009/136/CE.
19. La DCD de 2006 introdujo el apartado 1 *bis*. en el artículo 15 con dicha disposición (*Cfr*. art. 11 de la DCD). Por lo que el artículo 15.1 de la Directiva *e-Privacy* en su versión de 2006 modificada por la DCD se mantuvo solo con tres razones: «seguridad nacional», «defensa» y «seguridad pública».
20. RODOTÀ, S. (2006). «La conservación de los datos...», *op. cit*., pág. 57.

© 2021, Andoni Polo Roca
© de esta edición: 2021, Universitat Oberta de Catalunya

2.3. La Ley de Conservación de Datos (2007)

Por su parte, la Ley de Conservación de Datos (LCD) fue la norma que traspuso la DCD al ordenamiento jurídico español, estableciendo lo mismo que esta en cuanto al objeto (art. 1.1 de la LCD) y en relación con los datos que debían conservarse (art. 3 de la LCD).

En cuanto al plazo de conservación[21], según la LCD, los datos de tráfico deberán conservarse durante un plazo de doce meses, computados desde la fecha en que se haya producido la comunicación, ampliables reglamentariamente hasta un máximo de dos años y reducibles hasta un mínimo de seis meses (art. 5.1); decisión que se basa en criterios como el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave, previa consulta de los operadores[22].

Por otro lado, para acceder a los datos conservados por los operadores (acceso a estos por las autoridades), tal como recogió la LCD, será siempre necesaria la «autorización judicial previa» (art. 6.1) –esto no lo recogió la DCD–, y los «agentes facultados» serán únicamente las Fuerzas y Cuerpos de Seguridad (cuando desempeñen funciones de policía judicial), la Dirección Adjunta de Vigilancia Aduanera y el Centro Nacional de Inteligencia (art. 6.2), a quienes los operadores deberán entregar los datos conservados.

3. La posición del TJUE

3.1. El caso *Digital Rights Ireland y Seitlinger y otros* (2014)

Todo este régimen construido por la DCD fue cuestionado por el TJUE en el caso *Digital Rights Ireland y Seitlinger y otros*[23] del año 2014.

Según el TJUE, la DCD, al establecer la «conservación generalizada e indiferenciada», abarcaba a todas las personas sin que se estableciera ninguna diferenciación, limitación o excepción en función del objetivo de lucha contra los delitos graves (§57); incluso sin que las personas cuyos datos se conservan se encuentren, ni siquiera indirectamente, en una situación que pueda dar lugar a acciones penales (§58).

El Tribunal de Luxemburgo declaró que la regulación de la DCD constituía una injerencia en los derechos fundamentales de respeto de la vida privada y familiar, y de protección de datos de carácter personal protegidos por la CDFUE (arts. 7 y 8) –a pesar de que no se conserve el contenido de las comunicaciones–, y de especial gravedad en el ordenamiento jurídico de la Unión, ya que la norma permitía la «conservación generalizada e indiferenciada», sin disposiciones que permitieran garantizar que la injerencia (la conservación) se limitaba efectivamente a lo estrictamente necesario (§ 65).

Según el TJUE, por tanto, no se daba la debida ponderación que exigen los derechos fundamentales en virtud de la CDFUE (art. 52.1). Si bien la lucha contra el terrorismo o la delincuencia grave es un motivo válido (al constituir un interés general de la Unión[24]), no cabe una «conservación generalizada e indiferenciada», sino una «conservación selectiva y limitada».

Concluyó el Tribunal afirmando que «el legislador de la Unión sobrepasó los límites que exige el respeto del principio de proporcionalidad» (sic) en relación con los derechos implicados (§69).

En suma, la DCD quedó totalmente invalidada, y dejó de estar vigente desde el 8 de abril de 2014.

Por último, es preciso resaltar un importante apunte que

21. Según lo dispuesto por la DCD, los Estados miembros podían optar por el período que creyesen conveniente en una horquilla de seis meses a dos años (art. 6).
22. CUBERO MARCOS, J. I. (2021). «Las normas dictadas en desarrollo del artículo 13 de la Directiva 95/46/CE, en especial la privacidad en las comunicaciones electrónicas». En: TRONCOSO REIGADA, A. (dir.). Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales. Tomo II. Cizur Menor (Navarra): Civitas-Thomson Reuters, págs. 4559-4586, pág. 4568; y VILASAU SOLANA, M. (2006). «La Directiva 2006/24/CE sobre conservación de datos del tráfico en las comunicaciones electrónicas: seguridad v. privacidad». *IDP. Revista de Internet, Derecho y Política*, núm. 3, 2006, pág. 4.
23. STJUE (Gran Sala) de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland y Seitlinger y otros*.
24. STJUE (Gran Sala) de 23 de noviembre de 2010, asunto C-145/09, *Land Baden-Württemberg contra Panagiotis Tsakouridis*, § 46 y 47.

© 2021, Andoni Polo Roca
© de esta edición: 2021, Universitat Oberta de Catalunya

hace el propio Tribunal en esta resolución: el hecho de que «la conservación de los datos y su posterior utilización se efectúen sin que el abonado o el usuario registrado hayan sido informados de ello puede generar en las personas afectadas el sentimiento de que su vida privada es objeto de una vigilancia constante» (§ 37); es decir, una vigilancia de datos, *dataveillance*, de la ciudadanía.

Como apunte final, tal como hemos expuesto en el anterior apartado, la DCD estableció que el artículo 15.1 de la Directiva *e-Privacy* no sería de aplicación al ámbito de los datos de la DCD (art. 11), pero al quedar la DCD invalidada, el artículo 15.1 de la Directiva *e-Privacy* y su habilitación en dichos datos recuperaron su vigencia inicial[25].

3.2. El caso *Tele2 Sverige y Watson y otros* (2016)

Al caso del año 2014, por otro lado, debemos añadirle otro pronunciamiento del TJUE: el caso *Tele2 Sverige y Watson y otros*[26] del año 2016, que siguió la doctrina del citado caso *Digital Rights Ireland y Seitlinger y otros*.

En esta ocasión, el Tribunal de Luxemburgo declaró que el Derecho de la Unión se opone a una legislación nacional que establece, con la finalidad de luchar contra la delincuencia, la (obligación de) «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 (§ 112).

A juicio del Tribunal, un Estado miembro puede hacer uso de la habilitación del artículo 15 de la Directiva *e-Privacy*, pero no en los términos en los que estaba configurado en la invalidada DCD de 2006 (conservación masiva e indiferenciada).

Asimismo, el Derecho de la UE también se opone a una normativa nacional que regula el acceso de las autoridades nacionales competentes a los datos conservados, sin limitar dicho acceso, en el marco de la lucha contra la delincuencia, a los casos de delincuencia grave, sin supeditar dicho acceso a un control previo por un órgano jurisdiccional o una autoridad administrativa independiente, y sin exigir que los datos de que se trata se conserven en el territorio de la Unión (§ 125).

De este modo, tal como declara el TJUE, el artículo 15 de la Directiva *e-Privacy* «no se opone a que un Estado miembro adopte una normativa que permita, con carácter preventivo, la conservación selectiva de datos de tráfico y de localización a efectos de la lucha contra la delincuencia grave, siempre que la conservación de los datos esté limitada a lo estrictamente necesario en relación con las categorías de datos que deban conservarse, los medios de comunicación a que se refieran, las personas afectadas y el período de conservación establecido» (§ 108); esto es, una «conservación selectiva y limitada».

Por tanto, en esta ocasión el Tribunal declara que no cabe la «conservación generalizada e indiferenciada» por parte de una normativa nacional, y tampoco el acceso a dichos datos sin limitación o sin el control previo por un órgano jurisdiccional o una autoridad administrativa independiente.

4. La invalidez de la DCD y las normas nacionales de transposición de los Estados miembros

4.1. Planteamiento

Después del pronunciamiento del TJUE en el caso *Digital Rights Ireland y Seitlinger y otros* de 2014, algunos autores defendieron que la LCD y demás normas nacionales de transposición seguían en vigor pese a la anulación total de la DCD, defendiendo que «entre una y otra no hay una relación de interdependencia», por lo que si bien la relación entre ambas «parte esencialmente de un principio de primacía, una vez entre en vigor la norma nacional respetuosa de aquélla, adquiere autonomía en cuanto respecta a su vigencia»[27]. Argüían, a su vez, que, declarada la inva-

25. *Cfr*. FERNÁNDEZ RODRÍGUEZ, J. J. (2016). «Los datos de tráfico de comunicaciones...», *op. cit.*, págs. 110 y 111; y, también, RODRÍGUEZ LAINZ, J. L. (2014). «Sobre la incidencia de la declaración de invalidez de la Directiva 2006/24/CE en la ley española sobre conservación de datos relativos a las comunicaciones». *Diario La Ley*, núm. 8.308.
26. STJUE (Gran Sala), de 21 de diciembre de 2016, asuntos acumulados C-203/15 y C-698/15, *Tele2 Sverige y Watson y otros*.
27. RODRÍGUEZ LAINZ, J. L. (2014). «Sobre la incidencia...», *op. cit.*

© 2021, Andoni Polo Roca
© de esta edición: 2021, Universitat Oberta de Catalunya

lidez de la DCD, «la posibilidad de los Estados miembros de regular un régimen de conservación de datos en base a lo facultado en el art. 15.1 permanece inalterada»[28]. Otros autores, por su parte, defendieron la pérdida de la vigencia de la LCD[29].

Con la decisión del TJUE del año 2016, sin embargo, no hubo duda sobre el fin de la vigencia de las normas nacionales de transposición, hasta el punto de afirmar que se había dado la «definitiva defenestración» de la LCD[30].

4.2. ¿Pérdida de la vigencia de la LCD?

Como uno de los actos jurídicos de la UE, la directiva conlleva una obligación de resultado, dejando a los Estados miembros la elección de la forma y de los medios (art. 288 del TFUE); por lo que la forma dependerá de estos, pero el fondo o contenido básico será el marcado por la UE. Lo demás daría lugar a una transposición incorrecta con supuestos tales como: la divergencia regulatoria, la doble regulación, el deslizamiento regulatorio o la sobrerregulación[31].

Así, si bien es cierto que entre directiva y norma de transposición no hay una «interdependencia» plena, el contenido de esta será el de aquella, independientemente de la regulación «extra» que el Estado miembro haya añadido (sin caer en supuestos de transposición incorrecta, y sin que dicha regulación añadida por el Estado miembro modifique en esencia la Directiva traspuesta).

En el año 2014 el TJUE anuló la DCD por completo (caso *Digital Rights Ireland y Seitlinger y otros*), con su contenido, y ello afectó de forma directa a la LCD, ya que la función de la ley de transposición es incluir la regulación material de la norma europea y fue precisamente el «fondo» lo que fue declarado nulo por el Tribunal. Así, podemos explicarlo con una especie de «teoría del fruto del árbol envenenado»[32]: cuando el árbol está viciado (la DCD) los frutos que dé dicho árbol también lo estarán (las normas de transposición de los Estados miembros).

A ello le debemos añadir el supuesto fáctico de uno de los dos asuntos del caso *Tele2 Sverige y Watson y otros* del año 2016[33]: el proveedor sueco de servicios de comunicaciones electrónicas Tele2 Sverige notificó el 9 de abril de 2014 (día posterior a la sentencia del caso *Digital Rights Ireland y Seitlinger y otros*) a la autoridad sueca de control de los servicios de correos y telecomunicaciones que no seguiría conservando los datos de comunicaciones electrónicas y que suprimiría los conservados hasta esa fecha, interpretando la mencionada sentencia del año 2014. El Gobierno sueco, en cambio, estimó que se trataba de una interpretación incorrecta de la sentencia y que la legislación sueca de conservación de datos (que recogía el contenido de la DCD) no era contraria al Derecho europeo, especialmente al estar bajo el artículo 15.1 de la Directiva *e-Privacy* (el mismo punto de vista que mantuvo la gran parte de la doctrina para con la LCD española desde 2014 hasta 2016[34]).

El TJUE no hizo un pronunciamiento expreso de si las normas nacionales de transposición seguían en vigor o no después de la sentencia del año 2014, pero sí puso de manifiesto lo siguiente: el Derecho de la Unión no se

28. *Ibid*.
29. ENCINAR DEL POZO, M. Á. (2014). «La invalidez de la Directiva sobre Conservación y Cesión de los Datos relativos a las Comunicaciones». *Top Jurídico, Nuevas Tecnologías*. SEPIN; y, también, CUBERO MARCOS, J.L. (2021). «Las normas dictadas en desarrollo del artículo 13 de la Directiva 95/46/ CE, en especial la privacidad en las comunicaciones electrónicas», *op. cit*., págs. 4572 a 4574.
30. RODRÍGUEZ LAINZ, J. L. (2017). «La definitiva defenestración de la Ley Española sobre conservación de datos relativos a las comunicaciones». *Diario La Ley,* núm. 8.901.
31. RENDA, A. (2009). *Policy-making in the EU: achievements, challenges and proposals for reform.* Bruselas: Centre for European Policy Studies (CEPS), págs. 76 y 77.
32. Esta teoría es utilizada en el derecho procesal para hacer referencia a las pruebas obtenidas de manera ilícita; la metáfora, no obstante, es aplicable a este caso. Ello tiene su origen o referencia en las escrituras bíblicas: *Cfr*. Mateo 7:17-20.
33. La sentencia *Tele2 Sverige y Watson y otros* tuvo dos asuntos acumulados: el asunto C-203/15 y el asunto C-698/15. En este caso preciso se hace referencia al asunto C-203/15.
34. RODRÍGUEZ LAINZ, J. L. (2014). «Sobre la incidencia...», *op. cit.;* y, también, FERNÁNDEZ RODRÍGUEZ, J. J. (2016). «Los datos de tráfico de comunicaciones...», *op. cit.*, págs. 110 y 111: «téngase en cuenta que la Directiva 2002/58/CE sigue en vigor, por lo que el derecho comunitario continúa posibilitando que se establezca un régimen excepcional de conservación de datos, a la que pueden acudir los Estados para su regulación».

© 2021, Andoni Polo Roca
© de esta edición: 2021, Universitat Oberta de Catalunya

opone a que los Estados miembros adopten medidas legislativas *ex* artículo 15.1 de la Directiva *e-Privacy*, pero no en los términos en los que estaban *ex* transposición de la DCD («conservación generalizada e indiferenciada», sin limitación); por lo que el Tribunal da a entender que las normas de transposición de la DCD resultaron contrarias al Derecho de la UE desde el caso *Digital Rights Ireland y Seitlinger y otros* de 2014.

Por tanto, se podría inferir que la LCD perdió su vigencia el 8 de abril de 2014, mas esta cuestión está muy lejos de ser pacífica.

5. La posición del Tribunal Supremo: LCD en vigor

Con todo lo dicho hasta aquí, el Tribunal Supremo (TS) ha rechazado la pérdida de la vigencia de la LCD, declarándola aplicable y vigente en su totalidad.

En primer lugar, el TS pone de manifiesto que la LCD de 2007 recoge la autorización judicial previa necesaria (art. 6.1), lo que no constituía una garantía con la DCD[35].

A ello el Tribunal le añade una especie de «juego de fechas»: la sentencia *Digital Rights Ireland y Seitlinger y otros* fue dada el 8 de abril de 2014 (08-04-2014), y, en España, la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (LGT) entró en vigor el 11 de mayo de 2014[36] (11-05-2014). Así, el artículo 42 de la LGT se remite a la LCD de 2007, sin tener en cuenta los problemas derivados de la declaración de nulidad de la DCD por parte del TJUE; una ley (LGT) que es posterior a la sentencia del TJUE[37].

Además, toma en consideración otra premisa: el artículo 588 *ter* j de la LECrim fue creada e introducida en la LECrim por la Ley Orgánica 13/2015, de 5 de octubre, que entró en vigor el 6 de diciembre de 2015[38] (06-12-2015). Dicho artículo recoge la cesión (con autorización judicial) de los datos de comunicaciones electrónicas conservados por los operadores de telecomunicaciones, partiendo de la base de la legislación sobre conservación de datos relativos a las comunicaciones electrónicas (es decir, la LCD). Por lo que también la LO 13/2015, que es posterior a la sentencia del TJUE, viene a reconocer la vigencia de la LCD, según el Tribunal.

Por tanto, a juicio del TS, «desde el punto de vista del derecho interno la situación normativa no ha variado» (sic)[39].

El TS también hace referencia a la sentencia *Tele2 Sverige y Watson y otros*, al ser de fecha de 21 de diciembre de 2016. Y a ella le responde argumentando que las exigencias del TJUE en dicho caso «están sujetas a la autorización de una autoridad independiente de la administrativa cual es la judicial», al recoger la LCD la necesaria autorización judicial previa (art. 6.1), por lo que, en palabras del Tribunal, «en principio no parece incompatible con la exigencia de una normativa nacional que no admita 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»[40].

Cierto es que ello cumpliría una de las exigencias del TJUE: la existencia de un control previo por un órgano jurisdiccional en el acceso a los datos conservados[41] (art. 6.1 de la LCD); no obstante, no cumpliría la otra exigencia del Tribunal: que una norma nacional no puede establecer una «conservación generalizada e indiferenciada»[42], y la LCD sí lo hace (arts. 1.1, 1.2, 2, 3 y 4 de la LCD).

Con todo, hasta la fecha, el Tribunal Supremo ha seguido manteniendo este criterio jurisprudencial en torno a la vigencia de la LCD[43].

35. STS 1594/2017, de 18 de abril, Ponente Excmo. Sr. D. Juan Saavedra Ruiz, FJ 2.º, apdo. n.º 2.6.
36. Véase: BOE núm. 114, de 10 de mayo de 2014.
37. STS 2800/2017, de 1 de junio, Ponente Excmo. Sr. D. Juan Saavedra Ruiz, FJ 3.º, apdo. n.º 2.5.
38. Véase: BOE núm. 239, de 6 de octubre de 2015.
39. STS 1594/2017, de 18 de abril, Ponente Excmo. Sr. D. Juan Saavedra Ruiz, FJ 2.º, apdo. n.º 2.6.
40. STS 2800/2017, de 1 de junio, Ponente Excmo. Sr. D. Juan Saavedra Ruiz, FJ 3.º, apdo. n.º 2.5.
41. *Cfr*. STJUE, *Tele2 Sverige y Watson y otros,* § 125.
42. *Cfr*. STJUE, *Tele2 Sverige y Watson y otros,* § 112.
43. Véanse, por todas: STS 110/2019, de 23 de enero, ponente Excma. Sra. D.ª Ana María Ferrer García, FJ 1.º, apdo. n.º 1; y STS 1966/2020, de 15 de junio, ponente Excmo. Sr. D. Andrés Martínez Arrieta, FJ 1.º.

© 2021, Andoni Polo Roca
© de esta edición: 2021, Universitat Oberta de Catalunya

6. La jurisprudencia posterior del TJUE: el artículo 15.1 de la Directiva *e-Privacy*

6.1. Caso *Ministerio Fiscal* (2018)

Entre la jurisprudencia posterior del Tribunal de Luxemburgo en relación con la conservación de datos de comunicaciones electrónicas, es preciso mencionar el caso *Ministerio Fiscal* del año 2018[44].

En este caso, el TJUE declaró que la habilitación de «prevención, investigación, descubrimiento y persecución de delitos» del artículo 15.1 de la Directiva *e-Privacy* no está limitado únicamente a la lucha contra los casos de «delincuencia grave», sino que se refiere a los «delitos» en general (§ 53).

Así, si bien el TJUE ha declarado que en lo que respecta a la habilitación de «prevención, investigación, descubrimiento y persecución de delitos» solamente la lucha contra la «delincuencia grave» puede justificar el acceso a dichos datos (§ 54), el Tribunal motivaba esa interpretación basándose en la ponderación entre objetivo perseguido y medida (§ 55).

Por tanto, conforme al principio de proporcionalidad, en el ámbito de la «prevención, investigación, descubrimiento y persecución de delitos» solo puede justificar una injerencia «grave» (en los derechos fundamentales) el objetivo de luchar contra la delincuencia que a su vez esté también calificada de «grave» (§ 56); 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» (§ 57).

Lo que viene a establecer el TJUE en este caso es que el acceso de las autoridades públicas a los datos de comunicaciones electrónicas puede darse para la «prevención, investigación, descubrimiento y persecución» de cualquier delito, sea «grave» o «general». Sin embargo, la injerencia en los derechos fundamentales (el acceso) solo podrá ser «grave» cuando el delito sea también «grave»; y, en cambio, cuando el delito no sea «grave», sino «general», la injerencia (el acceso) deberá ser «leve» (o «no grave»). Así, el umbral de gravedad del delito delimitará la medida y carácter de la injerencia.

Ello responde a la debida ponderación de los derechos fundamentales en conflicto (art. 52.1 de la CDFUE), debiendo ser proporcional el acceso (la injerencia) y el delito.

El acceso a los datos en virtud de la habilitación del artículo 15.1 de la Directiva *e-Privacy* se dará, por tanto, con cualquier delito, sin necesidad de que sea «delincuencia grave».

Por otro lado, el TJUE, en este caso, no entra a determinar qué debe entenderse por delincuencia grave como criterio ponderativo, y parece que lo deja en manos de los Estados miembros, según apunta parte de la doctrina[45].

Cabe señalar, por último, que, a la hora de resolver este caso, en el que el litigio provenía de España, el TJUE se remitió a la LCD, sin hacer ningún comentario sobre su aplicabilidad o vigencia; resulta un hecho bastante relevante que el propio Tribunal aplique una norma nacional que traspuso una Directiva anulada por él mismo (especialmente cuando precisamente su aplicabilidad era lo que estaba en duda) y que recoge una conservación reprobada por el Tribunal (v. § 12, § 21 y § 38).

6.2. Caso *Privacy International y otros* (2020)

Por otro lado, entre las resoluciones en este ámbito, encontramos también el caso *Privacy International y otros* del año 2020[46], en relación con la «transmisión generalizada e indiferenciada» de este tipo de datos y la seguridad nacional.

En este caso, el TJUE resolvió que está comprendida en el ámbito de aplicación de la Directiva *e-Privacy* (siendo aplicable su artículo 15.1) una normativa nacional que permite a una autoridad estatal obligar a los proveedores

44. STJUE (Gran Sala), de 2 de octubre de 2018, asunto C-207/16, *Ministerio Fiscal*.
45. *Cfr*. OROMÍ I VALL-LLOVERA, S. (2020). «Acceso a datos personales conservados por proveedores de servicios de comunicaciones electrónicas en investigaciones penales según el Tribunal de Justicia de la UE». *IDP. Revista de Internet, Derecho y Política,* núm. 31, págs. 1-13, pág. 6.
46. STJUE (Gran Sala), de 6 de octubre de 2020, asunto C-623/17, *Privacy International y otros*.

© 2021, Andoni Polo Roca
© de esta edición: 2021, Universitat Oberta de Catalunya

de servicios de comunicaciones electrónicas a transmitir a las agencias de seguridad e inteligencia datos de tráfico y de localización con el fin de proteger la seguridad nacional (§ 49).

Por tanto, bajo la aplicación del artículo 15.1 de la Directiva están la «conservación», el «acceso» y la «transmisión» (§ 39 y 49), todos ellos distintos niveles de injerencia en los derechos fundamentales.

De este modo, el Tribunal establece que, siendo de aplicación el artículo 15.1, este se opone a una normativa nacional que permite a una autoridad estatal obligar a los proveedores de servicios de comunicaciones electrónicas a realizar una «transmisión generalizada e indiferenciada» de datos de tráfico y de localización a las agencias de seguridad e inteligencia con el fin de proteger la seguridad nacional (§ 82), ya que ello excede de los límites de lo estrictamente necesario y no puede considerarse justificada en una sociedad democrática (§ 81), faltando a la ponderación debida (art. 51.1 de la CDFUE).

Ello sigue la doctrina del caso *Digital Rights Ireland y Seitlinger y otros*: cuando es «generalizada e indiferenciada» no caben ni «conservación», ni «acceso», ni «transmisión», sin las debidas limitaciones, garantías y exigencias.

6.3. Caso *La Quadrature du Net y otros contra Premier ministre y otros* (2020)

A todo lo mencionado hasta aquí debemos añadirle el caso *La Quadrature du Net y otros contra Premier ministre y otros* del año 2020[47]. En esta decisión, el TJUE aprovechó para sentar doctrina sobre cómo ha de interpretarse la habilitación especial del artículo 15.1 de la Directiva *e-Privacy* (anteriormente mencionada), con qué límites. Por ello, aunque pueda parecer que el Tribunal avala la «conservación generalizada e indiferenciada» de los datos de comunicaciones electrónicas, en realidad hace justo lo contrario: establece las bases, límites y situaciones tasadas en las que puede tener cabida, pero deja en todo momento claro que la norma general es su incompatibilidad con el Derecho de la UE, ratificando su doctrina de 2014 y 2016.

Así, en primer lugar, el TJUE establece cuál es la norma general en este ámbito: el artículo 15.1 de la Directiva *e-Privacy* se opone a las medidas legislativas que, a los efectos establecidos en dicho artículo, prevén, como medida preventiva, la «conservación generalizada e indiferenciada» de los datos de comunicaciones electrónicas (§ 168).

Sin embargo, continúa el Tribunal, el artículo 15.1 no se opone a medidas legislativas que permitan recurrir a un requerimiento efectuado a los prestadores de comunicaciones electrónicas para que procedan a una «conservación generalizada e indiferenciada», en situaciones de una amenaza grave para la seguridad nacional (que sea real y actual o previsible), cuando esté sujeto a revisión efectiva y solo por un período limitado a lo «estrictamente necesario» (§ 168).

Asimismo, tampoco se opone a aquellas medidas legislativas que, con base en la seguridad nacional, la lucha contra delitos graves o la prevención de amenazas graves para la seguridad pública, prevean (§ 168): la «conservación selectiva» y delimitada de datos de comunicaciones electrónicas, por un período limitado a lo «estrictamente necesario»; la «conservación generalizada e indiferenciada» de las direcciones IP, por un período limitado a lo «estrictamente necesario»; la «conservación generalizada e indiferenciada» de datos relacionados con la identidad civil de los usuarios de comunicaciones electrónicas; o un requerimiento a los operadores para que procedan a la conservación urgente o rápida de los datos por un período de tiempo determinado y sujeto a revisión judicial efectiva.

Por otro lado, el artículo 15.1 no se opone a las normas nacionales que exigen que los proveedores de servicios de comunicaciones electrónicas recurran: en primer lugar, al análisis automatizado, cuando se limita a situaciones de una amenaza grave para la seguridad nacional (que sea real y actual o previsible), y cuando esté sujeta a revisión efectiva; y, en segundo lugar, a la recopilación en tiempo real de datos técnicos relativos a la ubicación cuando se limita a las personas respecto de las cuales exista una razón válida para sospechar que están implicadas de una

47. STJUE (Gran Sala), de 6 de octubre de 2020, asuntos acumulados C-511/18, C-512/18 y C-520/18, *La Quadrature du Net y otros contra Premier ministre y otros*.

© 2021, Andoni Polo Roca
© de esta edición: 2021, Universitat Oberta de Catalunya

forma u otra en actividades terroristas y está sujeto a una revisión previa (§ 192)[48].

Además, según el TJUE, un órgano jurisdiccional nacional no puede aplicar una disposición nacional que le faculta para limitar en el tiempo los efectos de una declaración de ilegalidad (que le correspondería efectuar según su Derecho nacional) con respecto a una normativa nacional que impone, que impone –con miras, en particular, a la protección de la seguridad nacional y de lucha contra la delincuencia– una obligación de «conservación generalizada e indiferenciada» de los datos de tráfico y de localización incompatible con el Derecho de la Unión; y, además, el juez penal nacional debe descartar las informaciones y las pruebas que se han obtenido a través de la «conservación generalizada e indiferenciada» de los datos de tráfico y de localización incompatible con el Derecho de la Unión (§ 227 y 228)[49].

Por tanto, en esta resolución, el TJUE sentó las bases de la conservación de datos, enumerando de modo exclusivo y excluyente los escenarios que pueden dar lugar a posibilitar la «conservación generalizada e indiferenciada», además de todas las garantías que deberán acompañar a ésta. No obstante, esta será siempre una excepción a la norma general del Derecho de la UE de prohibición de la «conservación generalizada e indiferenciada»; por ello, los Estados miembros solo podrán adoptar estas medidas en casos excepcionales, y no podrán recopilar datos de los ciudadanos de forma indiscriminada a través de los operadores de telecomunicaciones.

Después de este pronunciamiento del TJUE, algunos autores han defendido que se ha dado el «resurgimiento de regímenes de conservación preventiva de datos», entre ellos la *re-vigencia* o vuelta a la vigencia de la LCD[50].

No obstante, si bien podría parecer que esta decisión del Tribunal «refuerza» la LCD, no es así: la perjudica. Las exigencias del TJUE en el caso *La Quadrature du Net y otros contra Premier ministre y otros* relativos a la «conservación generalizada e indiferenciada» son: que sea una medida «excepcional», que haya una «amenaza grave para la seguridad nacional» (real y actual o previsible) u otro supuesto (seguridad pública, delincuencia grave, etc.), que sea por «período limitado» a lo «estrictamente necesario», etc.

La LCD, en cambio, no cumple ni una de ellas: es una medida general, sin haber amenaza (ni justificarla, ni recoger una lista) y por un período de doce meses (art. 5.1) –sí cumple, no obstante, la exigencia de autorización judicial previa (art. 6.1)–. Por ello, el TJUE vuelve a *arrollar* a la LCD; es más, no solo a la LCD, sino que dicho fallo obligó a los países partes en el proceso a modificar sus legislaciones (objeto de litigio).

Asimismo, por último, lo declarado por el TJUE respecto de los órganos jurisdiccionales nacionales y del juez penal nacional hace tambalear el artículo 588 *ter* j de la LECrim introducida en el año 2015.

6.4. Caso *H.K. v Prokuratuur* (2021)

Por último, nos es menester hacer referencia al caso *H.K. v Prokuratuur* del año 2021[51].

En este caso, el TJUE vuelve a recordar que el Derecho de la Unión y, en especial, el artículo 15.1 de la Directiva *e-Privacy* se opone (como norma general) a medidas legislativas que establezcan, para la prevención, la investigación, el descubrimiento y la persecución de delitos, la «conservación generalizada e indiferenciada», con carácter preventivo, de los datos de comunicaciones

48. Así, en este caso debe haber lo que el Derecho español denomina «indicios racionales de criminalidad», ya que, si no los hubiera, no habría una ponderación debida, y habría una intromisión desproporcionada en los derechos fundamentales.
49. En el derecho procesal, esta es la llamada «teoría del fruto del árbol envenenado». Véanse: artículo 11 de la LOPJ, STC 114/1984, de 29 de noviembre, y STS 5439/2002, de 18 de julio, rec. n.º 3269/2000, FJ 3.º.
50. Véase: RODRÍGUEZ LAINZ, J. L. (2020). «¿El renacer de la Ley española sobre conservación de datos relativos a las comunicaciones? (Comentario a la STJUE, Gran Sala, de 6 de octubre de 2020)». *Diario La Ley*, núm. 9.740. El autor defiende que la LCD, interpretada a la luz de este pronunciamiento, podría hacer que ésta fuera aplicable. No obstante, ello supone «hilar muy fino»: salvar unas pocas disposiciones de la LCD mediante una interpretación que se adecúe a este fallo del TJUE no supone un nivel adecuado de seguridad jurídica en el día a día de la aplicación de la norma.
51. STJUE (Gran Sala), de 2 de marzo de 2021, asunto C-746/18, *H.K. v Prokuratuur.*

© 2021, Andoni Polo Roca
© de esta edición: 2021, Universitat Oberta de Catalunya

electrónicas (§ 30). Se sigue, además, la doctrina de los casos *Ministerio Fiscal* (2018) y *La Quadrature du Net y otros* (2020): el umbral de gravedad del delito delimita la medida y carácter de la injerencia (§ 33).

En lo que respecta al objeto de análisis, el TJUE vuelve a pronunciarse sobre los requisitos que debe cumplir cualquier regulación sobre conservación de datos (§ 48): para cumplir el requisito de proporcionalidad, una normativa de este tipo debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas, y debe indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de tales datos.

Todo ello vuelve a hacer el contra de la LCD española, ya que, como hemos analizado, el régimen que recoge no cumple los requisitos que el TJUE exige: reglas claras y precisas, exigencias mínimas, circunstancias, requisitos, etc.

Cabe comentar, por último, que la futura Ley General de Telecomunicaciones (2021) recoge el contenido idéntico del anteriormente mencionado artículo 42 de la LGT de 2014, y entrará en vigor con fecha posterior a estos pronunciamientos del TJUE[52]. Por tanto, después de analizar la posición del TS, es posible que el TS siga manteniendo su postura respecto a la vigencia de la LCD, fundamentándola en el «juego de fechas», al entrar en vigor la nueva LGT (2021) con posterioridad a estos pronunciamientos del TJUE.

No obstante, las fechas de entrada en vigor de una norma o de un pronunciamiento, o la relación cronológica de ambas, es un elemento meramente formal, lejos de lo que es el fondo de la cuestión: la regulación misma de la LCD.

7. Conclusiones

De todo lo analizado hasta aquí se desprende que el debate en torno a la regulación sobre conservación de datos de comunicaciones electrónicas está muy lejos de acabar.

La doctrina apunta en distintas direcciones en torno a la LCD; el TS, en cambio, la considera totalmente aplicable y en vigor; y, por su parte, el TJUE dio a entender que las leyes nacionales de transposición de la DCD eran contrarias al Derecho de la UE en su resolución del año 2016 (lo cual parecía indicar que la LCD quedaba «defenestrada»), pero sigue aplicando la LCD a la hora de resolver litigios como hemos visto en sus resoluciones de 2018 y 2020.

En este contexto es evidente la incertidumbre que todo ello genera, y esta inseguridad jurídica afecta directamente a los operadores de telecomunicaciones, ya que, si la LCD resulta aplicable y no conservaran los datos, incumplirían la LCD y, en cambio, si la LCD resulta no aplicable y los conservaran, incumplirían la Directiva *e-Privacy,* además de la normativa en materia de protección de datos (en esa situación se encontró la compañía sueca Tele2 Sverige, como hemos mencionado). Todo ello resulta bastante farragoso o difuso también en lo que respecta al cumplimiento normativo o *compliance* en este ámbito.

De todo lo analizado se puede deducir con pocas dudas que la LCD resulta inaplicable en los términos actuales (*ex* DCD): es la transposición de una directiva anulada, que no se ha reformado en todos estos años y que, a la luz de todos los pronunciamientos del TJUE, no cumple los requisitos del Derecho de la UE, y ha sido, y es, «defenestrada» cada vez que el TJUE se pronuncia y completa su doctrina en este ámbito. No obstante, no es menos cierto que en la práctica judicial el TS considera aplicable y vigente tanto la LCD como los preceptos correspondientes de la LGT y LECrim, por lo que, siguiendo la posición del TS, parece que deberá ser aplicada a la hora de resolver litigios.

A ello se le añade, asimismo, las cuantiosas inversiones que las compañías de comunicaciones electrónicas se vieron obligadas a realizar en el año 2007 en virtud de la LCD en la infraestructura técnica necesaria para poder conservar los mencionados datos (*software*, so-

52. Véase: Anteproyecto de Ley General de Telecomunicaciones. Artículo 61. Conservación y cesión de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

© 2021, Andoni Polo Roca
© de esta edición: 2021, Universitat Oberta de Catalunya

portes de almacenamiento para su disponibilidad, etc.), y otros factores (sanciones posibles, reputación corporativa, etc.)[53].

Por otro lado, en términos generales sobre la conservación de datos, el TJUE parece que ha ido moldeando su doctrina sobre ésta en sus decisiones de los años 2014 y 2016 y sus posteriores, como la de 2020 o la de 2021, siguiendo siempre un criterio fundamental (como norma general): el Derecho de la UE se opone a normativas (europeas o nacionales) de «conservación generalizada e indiferenciada» de todos los datos de comunicaciones electrónicas.

De este modo, a lo manifestado por el TJUE en el caso *La Quadrature du Net y otros contra Premier ministre y otros* (2020) y en el caso *H.K. v Prokuratuur* (2021) debemos añadirle también el caso *Schrems II* de 2020[54], dado que de las posiciones que está manteniendo el TJUE se deduce una preocupación por la conservación y acceso masivo a datos bajo el pretexto de la seguridad nacional; por ello, el Tribunal ha querido coger la delantera y sentar las bases de esta regulación.

Concluimos, por todo ello, resaltando el hecho de que no estaría de más que el legislador español elaborase una nueva ley que sucediera a la ya «mareada» LCD de 2007 (que a la luz del Derecho de la UE resulta inaplicable), especialmente al estar ante un ámbito tan peligroso para la privacidad de la ciudadanía; una ley que sea capaz de conjugar seguridad y privacidad, y en la que, de *lege ferenda*, «el legislador [no sobrepase] los límites que exige el respeto del principio de proporcionalidad» (sic).

53. Mi más sincero agradecimiento a D. Daniel Escoda Villacorta por su cercanía y su ayuda, y por ofrecerme el punto de vista práctico del día a día tan necesario, que me ha permitido abordar este análisis también desde otras perspectivas.

54. STJUE (Gran Sala), de 16 de julio de 2020, asunto C-311/18, *Data Protection Commissioner contra Facebook Ireland Limited y Maximillian Schrems*.

© 2021, Andoni Polo Roca
© de esta edición: 2021, Universitat Oberta de Catalunya

Referencias bibliográficas

CUBERO MARCOS, J. I. (2021). «Las normas dictadas en desarrollo del artículo 13 de la Directiva 95/46/CE, en especial la privacidad en las comunicaciones electrónicas». En: TRONCOSO REIGADA, A. (dir.). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales. Tomo II*. Cizur Menor (Navarra): Civitas-Thomson Reuters, págs. 4559-4586.

CUBERO MARCOS, J. I., ABERASTURI GORRIÑO, U. (2008). «Protección de los datos personales en las comunicaciones electrónicas: especial referencia a la Ley 25/2007, sobre conservación de datos». *Revista española de derecho constitucional,* vol. 28, núm. 83, págs. 175-197 [en línea] http://www.cepc.gob.es/publicaciones/revistas/revistaselectronicas?IDR=6&IDN=658&IDA=27128 [Fecha de consulta: 12 de enero de 2021].

ENCINAR DEL POZO, M. Á. (2014). «La invalidez de la Directiva sobre Conservación y Cesión de los Datos relativos a las Comunicaciones». *Top Jurídico, Nuevas Tecnologías*. SEPIN.

FERNÁNDEZ RODRIGUEZ, J. J. (2016). «Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente». *Revista española de derecho constitucional,* vol. 36, núm. 108, págs. 93-122 [en línea] DOI: https://doi.org/10.18042/cepc/redc.108.03 [Fecha de consulta: 12 de enero de 2021].

MILAJ, J. (2015). «Invalidation of the data retention directive: extending the proportionality test». *Computer Law& Security Review*, vol. 31, núm. 5, págs. 604-617 [en línea] DOI: https://doi.org/10.1016/j.clsr.2015.07.004 [Fecha de consulta: 12 de enero de 2021].

OROMÍ I VALL-LLOVERA, S. (2020). «Acceso a datos personales conservados por proveedores de servicios de comunicaciones electrónicas en investigaciones penales según el Tribunal de Justicia de la UE». *IDP. Revista de Internet, Derecho y Política*, núm. 31, págs. 1-13 [en línea] DOI: https://doi.org/10.7238/idp.v0i31.3206 [Fecha de consulta: 12 de enero de 2021].

RENDA, A. (2009). *Policy-Making in the EU: Achievements, Challenges and Proposals for Reform*. Bruselas: Centre for European Policy Studies (CEPS).

RODOTÀ, S. (2006). «La conservación de los datos de tráfico en las comunicaciones electrónicas». *IDP. Revista de Internet, Derecho y Política,* núm. 3, págs. 53-60 [en línea]. https://www.raco.cat/index.php/IDP/article/view/49964/50870 [Fecha de consulta: 12 de enero de 2021].

RODRÍGUEZ LAINZ, J. L. (2014). «Sobre la incidencia de la declaración de invalidez de la Directiva 2006/24/CE en la ley española sobre conservación de datos relativos a las comunicaciones». *Diario La Ley,* núm. 8.308.

RODRÍGUEZ LAINZ, J. L. (2017). «La definitiva defenestración de la Ley Española sobre conservación de datos relativos a las comunicaciones». *Diario La Ley*, núm. 8.901.

RODRÍGUEZ LAINZ, J. L. (2020). «¿El renacer de la Ley española sobre conservación de datos relativos a las comunicaciones? (Comentario a la STJUE, Gran Sala, de 6 de octubre de 2020)». *Diario La Ley,* núm. 9.740.

RUCZ, M.; KLOOSTERBOER, S. (2020). «Data retention revisited booklet». *European Digital Rights (EDRi)* [en línea] https://edri.org/wcontent/uploads/2020/09/Data_Retention_Revisited_Booklet.pdf [Fecha de consulta: 12 de enero de 2021].

SÁNCHEZ GUARIDO, A.; MADDIO MEDINA, A. (2020). «El TJUE reabre el debate entre privacidad o seguridad nacional». *Diario La Ley*, núm. 9.743.

© 2021, Andoni Polo Roca
© de esta edición: 2021, Universitat Oberta de Catalunya

TRACOL, X. (2017). «The judgment of the Grand Chamber dated 21 December 2016 in the two joint Tele2 Sverige and Watson cases: the need for a harmonised legal framework on the retention of data at EU level». *Computer Law& Security Review*, vol. 33, núm. 4, págs. 541-552 [en línea] DOI: https://doi.org/10.1016/j.clsr.2017.05.003 [Fecha de consulta: 12 de enero de 2021].

VILASAU SOLANA, M. (2006). «La Directiva 2006/24/CE sobre conservación de datos del tráfico en las comunicaciones electrónicas: seguridad v. privacidad». *IDP. Revista de Internet, Derecho y Política,* núm. 3 [en línea] *https://dialnet.unirioja.es/servlet/articulo?codigo=2119656* [Fecha de consulta: 12 de enero de 2021].

Cita recomendada

POLO ROCA, Andoni (2021). «La regulación sobre la conservación de datos en el sector de las comunicaciones electrónicas o telecomunicaciones: estado de la cuestión». *IDP. Revista de Internet, Derecho y Política,* núm. 33 (octubre). UOC [Fecha de consulta: dd/mm/aa] http://dx.doi.org/10.7238/idp.v0i33.373811

SOME RIGHTS RESERVED

Los textos publicados en esta revista están —si no se indica lo contrario— bajo una licencia Reconocimiento-Sin obras derivadas 3.0 España de Creative Commons. Puede copiarlos, distribuirlos y comunicarlos públicamente siempre que cite su autor y la revista y la institución que los publica (IDP. *Revista de Internet, Derecho y Política*; UOC); no haga con ellos obras derivadas. La licencia completa se puede consultar en: http://creativecommons.org/licenses/by-nd/3.0/es/deed.es.

Sobre el autor

Andoni Polo Roca
apoloro@icasv-bilbao.com
Abogado

Abogado. Graduado en Derecho con el Premio Extraordinario de Fin de Carrera (2018) y Mención de Excelencia por la Universidad del País Vasco-Euskal Herriko Unibertsitatea (UPV/EHU) y Máster Universitario en Acceso a la Abogacía por la UPV/EHU. Letrado del Ilustre Colegio de la Abogacía de Bizkaia (ICAB-BAEO).

ORCID: 0000-0002-2763-501X

© 2021, Andoni Polo Roca
© de esta edición: 2021, Universitat Oberta de Catalunya