El TJUE reabre el debate entre privacidad o seguridad nacional

Andrea Sánchez Guarido
Alicia Maddio Medina
Abogadas de Propiedad Industrial, Intelectual y Tecnología de Pérez-Llorca

Diario La Ley, Nº 9743, Sección Tribuna, 25 de Noviembre de 2020, **Wolters Kluwer**

Normativa comentada
Comentarios

Para contextualizar el análisis que se realiza en el presente artículo es importante tener en cuenta el contenido de los pronunciamientos citados en el párrafo anterior, y es que el TJUE ha establecido en dichas sentencias que el Derecho de la Unión es contrario a toda legislación nacional que imponga a un proveedor de servicios de comunicaciones electrónicas la obligación de conservar de manera general e indiscriminada los datos de tráfico y localización de sus usuarios. Aún más, el TJUE ha llegado a dicha conclusión incluso si la finalidad de dicha imposición es la de que se transfieran tales datos a las autoridades públicas para salvaguardar la seguridad nacional o controlar eficazmente la delincuencia.

I. Introducción

La retención y procesamiento de datos técnicos de las comunicaciones electrónicas lleva más de una década siendo tratado de manera desigual por el Parlamento europeo y por el TJUE ya que, mientras el primero pretende asegurar su registro para fines de seguridad nacional, control de las infraestructuras críticas o la persecución de delitos, el segundo, con una aproximación más garantista, está poniendo límites a dicha conservación de datos a través de diferentes resoluciones judiciales. En las sentencias más recientes, sobre todo la de 6 de octubre de 2020, el TJUE ha analizado el alcance de la Directiva 2002/58/CE (LA LEY 9590/2002) sobre la privacidad y las comunicaciones electrónicas (la «**Directiva**» o la «**Directiva sobre la privacidad y las comunicaciones electrónicas**») a la luz de su jurisprudencia anterior al respecto, así como de la Carta de Derechos Fundamentales de la Unión Europea (LA LEY 12415/2007) (la «**Carta**») y del Reglamento General de Protección de Datos (LA LEY 6637/2016) (el «**RGPD**»).

En particular, estas sentencias dan respuesta a las cuestiones prejudiciales elevadas por tribunales de Francia, Bélgica y Reino Unido, los cuales debían resolver las impugnaciones efectuadas sobre sus respectivas normativas nacionales en materia de conservación de datos de comunicaciones electrónicas. Concretamente, las autoridades de dichos Estados miembros ponían en duda el alcance de la Directiva sobre la privacidad, cuestión que será analizada en el apartado III del presente artículo.

Consecuentemente, la nueva resolución impacta directamente sobre la LCD, dado que el objeto de dicha norma es imponer a los operadores de telecomunicaciones la obligación de conservación durante, generalmente, un período de 12 meses, los datos de tráfico, localización e identificación de los usuarios de sus redes, obligación que es ahora cuestionada por el TJUE.

II. Antecedentes

Para fundamentar su pronunciamiento, el TJUE se apoya, principalmente, en sus sentencias de 8 de abril de 2014 (LA LEY 36312/2014) (1) (« ***Digital Rights Ireland*** ») y de 21 de diciembre de 2016 (LA LEY 180541/2016) (2) (« ***Tele2*** »). En el caso *Digital Rights Ireland*, las cuestiones prejudiciales que traen causa de la sentencia fueron elevadas por los tribunales de Irlanda y Austria. Dichos tribunales, respectivamente, cuestionaban la legalidad de las medidas legislativas irlandesas sobre la conservación de datos relativos a comunicaciones electrónicas, así como la compatibilidad de la Ley constitucional federal austriaca con la norma por la que se transponía la Directiva 2006/24/CE (LA LEY 3617/2006) sobre la conservación de datos generados o tratados en relación con la prestación de

servicios de comunicaciones electrónicas de acceso público o redes públicas de comunicaciones (la «**Directiva sobre la conservación de datos**» o la «**Directiva invalidada**»). Por su parte, en el caso *Tele2* las cuestiones prejudiciales objeto del pronunciamiento fueron planteadas por los tribunales de Suecia y Reino Unido, cuestionando la interpretación del artículo 15.1 de la Directiva sobre la privacidad y las comunicaciones electrónicas (LA LEY 9590/2002). En dichas sentencias, respectivamente:

> **(i)** Se declaró la invalidez de la Directiva sobre la conservación de datos, por ser contraria a los derechos fundamentales reconocidos en los artículos 7 (LA LEY 12415/2007) y 8 de la Carta (LA LEY 12415/2007) (intimidad y protección de datos personales); y
> **(ii)** se estableció las bases de lo que, posteriormente se ha confirmado a través de los recientes pronunciamientos, es decir, la inadmisibilidad de toda norma destinada a conservar, de manera generalizada e indiscriminada, datos de tráfico y localización.

Como es lógico, tras los sendos pronunciamientos del TJUE, varias voces (3) reflexionaron sobre la necesidad de modificar la LCD para adaptarla a la norma europea, más aún cuando el objetivo principal de dicha Ley era transponer la Directiva sobre la conservación de datos. Si bien el objeto del presente artículo no es llevar a cabo un análisis sobre los efectos que derivan de la declaración de invalidez de una directiva europea sobre la norma nacional que la transpone, no podemos obviar la importancia que, en este caso, la invalidez de la Directiva sobre la conservación de datos tiene —o debería tener- sobre la LCD. En este sentido, la invalidez de una directiva no supone, formalmente, la derogación automática de las normas nacionales de transposición, sin embargo, ya se ha puesto de manifiesto que el TJUE fundamenta dicha invalidez sobre la vulneración de ciertos derechos fundamentales reconocidos en la Carta. Así pues, el legislador español, ya en el año 2014 tenía motivos suficientes para modificar la LCD y adecuar su contenido al ordenamiento jurídico europeo y a la más reciente normativa en materia de protección de datos.

Asimismo, la declaración de invalidez de la Directiva sobre la conservación de datos tiene otro efecto que los Estados miembros han sorteado, que consiste en la retrotracción al ordenamiento jurídico europeo de la versión originaria de la Directiva sobre la privacidad y las comunicaciones electrónicas, en tanto que la Directiva invalidada tenía como finalidad la modificación de esta última. Como consecuencia de ello, los Estados miembros, a la hora de regular la conservación de datos de las telecomunicaciones, habrán de estar al contenido de la Directiva sobre la privacidad y las comunicaciones electrónicas y el ámbito de aplicación de la misma no podrá ponerse en duda, tal y como se analiza en el apartado siguiente.

III. Ámbito de aplicación de la Directiva sobre la privacidad y las comunicaciones electrónicas

En las cuestiones prejudiciales elevadas al TJUE, los tribunales remitentes cuestionaban el alcance de la Directiva sobre la privacidad y las comunicaciones electrónicas cuando estuviesen en juego factores relacionados con la seguridad nacional de los Estados miembros. El motivo por el que resulta particularmente relevante determinar si la Directiva es de aplicación sobre la normativa de los Estados miembros que regula la conservación de datos es porque esta prevé una serie de garantías que, en todo caso, tendrán que ser observadas por los legisladores nacionales a la hora de imponer ciertas obligaciones a los proveedores de servicios de comunicaciones electrónicas. Dichas garantías se erigen en torno al principio de confidencialidad reconocido en su artículo 5 (LA LEY 9590/2002), así como alrededor del régimen de excepcionalidad previsto en el artículo 15 y cuyo contenido analizaremos a continuación. En resumidas cuentas, si la Directiva es de aplicación, toda normativa nacional que afecte a la conservación de datos tendrá que redactarse a la luz de la misma, teniendo que descartarse automáticamente la conservación generalizada e indiscriminada de los mismos.

En este sentido, los legisladores francés, belga e inglés hallaban el fundamento jurídico para excluir sus normativas del ámbito de aplicación de la Directiva en el artículo 1.3 (LA LEY 9590/2002) de la misma, el cual excluye del mismo las actividades de los Estados miembros relativas a la seguridad pública, la defensa y la seguridad del Estado. Hay que añadir que, *a priori*, esta interpretación restrictiva del ámbito de aplicación de la Directiva podría tener sentido a la luz del artículo 4.2 Tratado de la Unión Europea (LA LEY 109/1994) («**TUE**»), que reconoce a los Estados miembros la competencia exclusiva para mantener el orden público dentro de sus territorios. No obstante, dichos preceptos no pueden ser interpretados en el sentido de que toda medida legislativa destinada a la protección de la seguridad nacional de un Estado miembro quede blindada ante la aplicación de la Directiva. A este respecto, recuerda el TJUE (4) que el art. 1.3 de la Directiva debe ser interpretado, conjuntamente, con el art. 3 (LA LEY 9590/2002) de la

misma el cual establece que esta desplegará sus efectos sobre toda norma que regule las comunicaciones electrónicas en la UE, independientemente de si su finalidad es salvaguardar la seguridad nacional.

Asimismo, el artículo 4.2 TUE (LA LEY 109/1994) deberá interpretarse a tenor de lo dispuesto en el artículo 15.1 de la Directiva (LA LEY 9590/2002) (5) , el cual faculta a los Estados miembros a adoptar medidas legales que puedan limitar, no anular, el derecho a la confidencialidad de las comunicaciones cuando tal limitación constituya una medida necesaria, proporcionada y apropiada para proteger la seguridad del Estado. Es evidente que, en el momento en el que el legislador europeo habilita un mecanismo excepcional a través del cual los Estados miembros pueden limitar el derecho a la confidencialidad de las comunicaciones, está presuponiendo, necesariamente, que todas las medidas legislativas nacionales que afecten a los proveedores de servicios de comunicaciones electrónicas están sujetas a la Directiva y que dicho régimen excepcional únicamente podrá hacerse valer bajo las circunstancias enunciadas.

> Los E. miembros podrán llevar a cabo cualquier actividad dirigida a preservar la seguridad dentro de su territorio, sin embargo, cuando se impongan a los afectados ciertas obligaciones, se estará entrando en un ámbito regido por la UE

Por consiguiente, los Estados miembros podrán llevar a cabo cualquier actividad dirigida a preservar la seguridad dentro de su territorio, sin embargo, cuando dichas actividades impongan a los afectados (en este caso, a los proveedores de servicios de comunicaciones electrónicas) ciertas obligaciones, se estará entrando en un ámbito regido por el Derecho de la UE.

No podemos olvidar que la finalidad de cualquier directiva o reglamento es armonizar la legislación y las políticas de los Estados miembros y así evitar que se produzcan situaciones de desigualdad para los ciudadanos y los propios Estados dentro de la Unión Europea. En este sentido, el alcance de la normativa comunitaria no puede quedar al arbitrio de la interpretación que decidan darle algunos Estados miembros, siendo este alcance o ámbito de aplicación un elemento objetivo.

IV. Límites a la exigencia de conservación generalizada e indiscriminada de datos

Si bien el TJUE no pone en duda la potestad de los Estados para garantizar la seguridad dentro de su territorio, recuerda que la Directiva no autoriza a adoptar medidas legislativas que, de forma generalizada e indiscriminada, restrinjan los derechos y obligaciones previstos en la misma, a menos que dichas medidas respeten los principios generales del Derecho de la Unión.

Llegados a este punto resulta particularmente relevante recordar que el objetivo de la Directiva sobre la privacidad y las comunicaciones electrónicas es garantizar el derecho a la intimidad en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas y de los datos asociados a ellas. Dicho objetivo se erige, principalmente, en torno al principio de confidencialidad reconocido en el artículo 5 de la Directiva (LA LEY 9590/2002), que deberá ser garantizado por los Estados miembros a través de la legislación nacional. El TJUE dictamina que, para que la restricción de este derecho pueda estar justificada al amparo de la normativa comunitaria, el Estado miembro debe enfrentarse a una «amenaza grave» para la seguridad nacional que resulte ser «auténtica y presente» o, en su caso, «previsible».

En particular, los Estados miembros podrán exigir a los proveedores de servicios electrónicos la conservación y transmisión de datos de manera generalizada e indiscriminada bajo las siguientes circunstancias:

(i) Cuando la vigencia de la medida legislativa esté limitada en el tiempo;
(ii) En caso de que la restricción de derechos se circunscriba a lo estrictamente necesario para los fines perseguidos;
(iii) Cuando dichas medidas vayan acompañadas de las salvaguardas efectivas; y
(iv) En el supuesto de que un tribunal o una autoridad administrativa independiente revise que la medida cumple con lo anterior.

De igual modo, el TJUE expone que la Directiva interpretada a la luz de la Carta, reconoce a los Estados miembros la posibilidad de exigir a los proveedores de servicios de comunicación electrónicos la recopilación en tiempo real de datos de tráfico y localización de usuarios específicos cuando sobre los mismos recaiga una sospecha fehaciente de su participación en actividades terroristas. No obstante, el TJUE señala que en estos supuestos también se requerirá que la medida haya sido revisada por un tribunal o autoridad administrativa independiente de manera previa a su

entrada en vigor.

Por último, el alto tribunal europeo concluye que el artículo 15.1 de la Directiva (LA LEY 9590/2002) sobre la privacidad y las comunicaciones electrónicas debe ser interpretado a la luz del principio de efectividad. Dicho principio tiene como finalidad que los tribunales de los Estados miembros apliquen la normativa nacional garantizando que los derechos subjetivos reconocidos a los ciudadanos europeos puedan ser plena y eficazmente ejercidos por los mismos. Consecuentemente, los tribunales penales nacionales no podrán emplear la información y las pruebas que hayan sido obtenidas mediante la conservación general e indiscriminada de datos de tráfico y localización cuando para la recopilación de tales datos no se hayan observado los límites establecidos por el TJUE (limitación temporal de la medida, necesidad, garantías y revisión por autoridad judicial o administrativa). Como consecuencia de lo anterior, las sentencias analizadas, podrían, asimismo, desplegar sus efectos sobre la Ley de Enjuiciamiento Criminal (LA LEY 1/1882) («**LECrim**»). En particular, sobre el artículo 588.ter.j) (LA LEY 1/1882) que regula la incorporación al proceso penal de los datos de tráfico obrantes en archivos automatizados de los prestadores de servicios de comunicaciones electrónicas. Baste mencionar sucintamente que, en caso de que, efectivamente, el legislador español limite la obtención generalizada e indiscriminada de datos de forma preventiva, la disposición de la LECrim a la que nos referimos quedaría, *a priori*, vacía de contenido, precisamente porque los proveedores de servicios no podrían conservar tales datos en sus archivos.

V. Cómo afecta el fallo a la LCD

Como ha sido mencionado anteriormente, el objeto de la LCD es imponer a los operadores la obligación de conservación durante, generalmente, un período de 12 meses, —que podrá llegar a ampliarse hasta un máximo de dos años- de los datos de tráfico, localización e identificación de usuarios de sus redes de telecomunicaciones. Dicha obligación, prevista en el artículo 1.1. LCD (LA LEY 10470/2007), se establece de manera generalizada e indiscriminada sin que se impongan más limitaciones que la de contar con una previa autorización judicial para la cesión de los datos conservados.

Por consiguiente, el fallo del TJUE apela directamente a normativas como la española, puesto que, aunque el TJUE analiza normativa extranjera (en este caso, francesa, belga e inglesa), en el momento en el que ha puesto de manifiesto que tales disposiciones —redactadas en términos similares a los de la LCD- son contrarias al Derecho de la UE, no cabe sino deducir que la norma española también lo es.

> En caso de que el legislador español eluda la obligación de adaptar la normativa nacional a la comunitaria, la responsabilidad de aplicar dicha normativa de acuerdo con la jurisprudencia del TJUE recaería sobre los jueces nacionales

En consonancia con lo mencionado, si nuestro legislador quiere garantizar el derecho a la privacidad de los usuarios, tendrá que modificar sustancialmente la LCD y adaptarla a los principios reflejados en la Carta, así como al contenido de la Directiva sobre la privacidad y las comunicaciones electrónicas. Alternativamente, en caso de que el legislador español eluda la obligación de adaptar la normativa nacional a la comunitaria, la responsabilidad de aplicar dicha normativa de acuerdo con la jurisprudencia del TJUE recaería sobre los jueces nacionales.

VI. Conclusiones

A la luz de lo anterior, debemos entender que, si bien los Estados miembros son soberanos, los principios rectores de la Carta, y en este caso también del RGPD, deben estar presentes en todas las regulaciones nacionales y en todas las acciones que impliquen un acceso y posterior tratamiento de datos de carácter personal. El TJUE ha recordado una vez más que la inviolable seguridad del Estado no puede erigirse como comodín o excepción general para no cumplir en este caso con la Directiva y con cualquier otra norma que garantice la no menos importante intimidad y confidencialidad de la información, o imponga medidas que impliquen el registro indiscriminado de datos.

Los últimos pronunciamientos del TJUE en materia de privacidad (*Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems —C-311/18—)* nos llevan a pensar que existe una verdadera preocupación por parte del TJUE en relación con el acceso y el tratamiento masivo y sin justa causa de información de carácter personal o análoga que se llevan a cabo en diferentes países, amparados en cuestiones de seguridad nacional.

Aunque nadie niega la importancia que tiene la seguridad nacional, no debe olvidarse que tanto el derecho a la protección de datos como el derecho a la intimidad son derechos fundamentales que, si bien pueden ser objeto de

limitaciones cuando así lo requieran las circunstancias, no pueden obviarse de manera generalizada, sin, como ha recordado el TJUE, existir una amenaza grave, auténtica, presente o previsible.

(1) Sentencia en los asuntos acumulados C-293/12 (LA LEY 36312/2014) y C-594/12 Digital Rights Ireland y Seitlinger y otros.

(2) Sentencia en los asuntos acumulados C-203/15 (LA LEY 180541/2016) Tele2 Sverige AB / Post- och telestyrelsen y C-698/15 Secretaty of State for the Home Department/Tom Watson y otros.

(3) RODRÍGUEZ LAINZ, José Luís: «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» (LA LEY 2502/2014); «La definitiva defenestración de la Ley Española sobre conservación de datos relativos a las comunicaciones» (LA LEY 58/2017); y BALLESTEROS MOFFA, Luis Ángel, Revista Aranzadi de Derecho y Nuevas Tecnologías núm. 44/2017 «La difícil situación de la Ley 25/2007 de conservación y cesión de datos de tráfico y localización en las comunicaciones electrónicas: la tala de su base comunitaria y los desfavorables vientos de sus homólogas europeas»; entre otros.

(4) Párrafos 93 y 96 de la sentencia sobre los asuntos acumulados *La Quadrature du Net y otros* (C-511/18 y C-512/18), *Ordre des barreaux francophones et germanophone y otros* (C-520/18).

(5) Párrafo 87 y siguientes de la sentencia sobre los asuntos acumulados *La Quadrature du Net y otros* (C-511/18 y C-512/18), *Ordre des barreaux francophones et germanophone y otros* (C-520/18).