Revista de Derecho UNED, núm. 30, 2022

CONSECUENCIAS DE LA ANULACIÓN DE LA DIRECTIVA EUROPEA DE CONSERVACIÓN DE METADATOS DE LAS COMUNICACIONES ELECTRÓNICAS. UNA ENCRUCIJADA EN LA LUCHA CONTRA LA DELINCUENCIA GRAVE

CONSEQUENCES OF THE ANNULMENT OF THE EUROPEAN DIRECTIVE ON THE RETENTION OF METADATA IN ELECTRONIC COMMUNICATIONS. A CROSSROADS IN THE FIGHT AGAINST SERIOUS CRIME

Lorenzo Luna Zambrana

Doctorando en el Programa de Doctorado en Unión Europea (UNED)

Resumen: En 2006, la Unión Europea adoptó la Directiva 2006/24/CE, sobre conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público, para permitir a las agencias encargadas de la aplicación de la ley el acceso a los datos conservados de tráfico y localización que se generan en las comunicaciones electrónicas entre los ciudadanos

europeos (voz, datos e Internet), con fines (entre otros) de prevención y lucha contra la delincuencia grave. En 2014, la directiva fue declarada inválida por el Tribunal de Justicia de la Unión Europea (TJUE), por considerar que autorizaba una injerencia especialmente grave en los derechos fundamentales recogidos en los artículos 7 y 8 de la CDFUE[1], sin garantizar adecuadamente los principios de necesidad y proporcionalidad. A esta sentencia han seguido otras, que afectan también a las normas nacionales de transposición de la directiva europea. Todavía hoy no se ha encontrado una solución en el seno de las instituciones europeas. En este estudio, pretendemos establecer algunas claves que ayuden a resolver esta situación.

Palabras clave: Conservación de datos, cuestión prejudicial, delincuencia grave, derechos fundamentales, servicios policiales y autoridades judiciales.

Abstract: In 2006, the European Union adopted Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services, to allow law enforcement agencies access to retained traffic and location data generated in electronic communications between European citizens (voice, data and internet), for the purposes of (among others) preventing and combating serious crime. In 2014, the directive was declared invalid by the Court of Justice of the EU, on the grounds that it authorised a particularly serious interference with the fundamental rights enshrined in articles 7 and 8 of the ECHR, without adequately guaranteeing the principles of necessity and proportionality. This ruling has been followed by others, which also affect the national rules transposing the European directive. A solution has not yet been found within the European institutions. In this study, we aim to establish some keys to help resolve this situation.

Keywords: Data retention, preliminary rulings, serious crime, fundamental rights, law enforcement and judicial authorities.

Recepción original: 28/09/2022

Aceptación original: 14/11/2022

[1] Carta de los derechos fundamentales de la Unión Europea (2010/C 83/02), de 30 de marzo de 2010, en https://www.boe.es/doue/2010/083/Z00389-00403.pdf .

I. INTRODUCCIÓN

Los ciudadanos realizan cada vez más actividades y transacciones cotidianas utilizando redes y servicios de comunicaciones electrónicas (telefonía fija y móvil, Internet y, más recientemente, aplicaciones sobre IP), y todos y cada uno de los movimientos a través de estas redes generan una serie de datos que permiten a los proveedores de servicios cumplir con determinadas funciones administrativas y comerciales. Estos datos[2] también son importantes para los servicios policiales y las autoridades judiciales en la investigación y persecución de conductas delictivas graves o del terrorismo, máxime en un entorno político y geoestratégico como el actual —con múltiples amenazas y riesgos, clásicos y emergentes— en el que la seguridad nacional y la seguridad pública se han convertido en una prioridad de primer orden para las agendas políticas en la Unión Europea, de forma general; y de sus Estados miembros, de forma particular.

La dependencia de la sociedad actual de estas tecnologías ha derivado también en la necesidad de adaptar los marcos normativos hacia la mejora en la salvaguarda de la privacidad y de la protección de los datos de carácter personal, mediante consensos que no siempre han sido fáciles de alcanzar y con redacciones complejas, pero que han producido efectos positivos en la vida de los ciudadanos europeos y en la actividad de las personas jurídicas. Como contrapartida, han tenido igualmente una incidencia notable, muchas veces de forma negativa, en el trabajo de las autoridades policiales y judiciales en su labor de persecución del delito grave.

Ante una situación fragmentada en la que cada Estado miembro de la UE había aprobado su normativa nacional para regular el uso de estos datos —específicamente los datos de tráfico y de localización, dejando al margen el contenido de las comunicaciones, la Unión adoptó una directiva en 2006 que *obligaba* a los proveedores de servicios a conservar los datos generados por todos los usuarios y abonados y ponerlos a disposición de las autoridades competentes en la aplicación de la ley. No obstante, en 2014, el Tribunal de Justicia de la UE, en la sentencia del *Caso Digital Rights Ireland and Seitlinger y otros (C-293/12 y C-594/12)*, declaró nula la norma europea por no cumplir con los criterios de necesidad y proporcionalidad de las me-

[2] Entre los que se incluyen la hora, el lugar y los números utilizados para los servicios de voz fijos y móviles; correos electrónicos, mensajes de texto y otros cada vez más extendidos usos de Internet; o los datos de los abonados y, en ocasiones, de los usuarios, que incluyen el nombre, la dirección, la cuenta bancaria de pago, etcétera, y que son también tratados por los proveedores para la gestión de las suscripciones.

didas recogidas en la directiva y causar una injerencia desproporcionada en los derechos fundamentales de los ciudadanos. Desde entonces, el Tribunal europeo se ha pronunciado en diferentes momentos ante cuestiones prejudiciales planteadas por tribunales de algunos Estados miembros y ha confirmado su doctrina, con algunos matices concretos importantes. Al mismo tiempo, en el seno de las instituciones europeas se inició un proceso de reflexión, que todavía sigue hoy —aunque se encuentra en un punto muerto— para buscar una solución satisfactoria para las necesidades de los servicios policiales y otras autoridades competentes y, al mismo tiempo, cumplir con los requerimientos del Tribunal de Luxemburgo.

Es evidente para todos los actores implicados en este análisis y debate, que la nueva realidad jurídica ha situado en una encrucijada la labor de los servicios policiales y las autoridades judiciales en la prevención, persecución y enjuiciamiento de la delincuencia grave. Ocho años después (octubre de 2022), no se vislumbra de forma nítida un camino hacia un fin aceptado por todas las partes, lo que suma una pieza más al complejo *puzle* del dilema *seguridad vs. libertad*. En este estudio, como parte de una tesis doctoral, se pretende aportar algunos elementos concretos que ayuden en esa labor.

II. EL DILEMA SEGURIDAD VS. LIBERTAD

No parece estar en cuestión, al menos de forma generalizada, que la seguridad es clave para el desarrollo de una sociedad democrática. Hay dos vertientes extendidas y contrapuestas de la relación entre ambos conceptos: una considera que a mayor seguridad se produce una mayor garantía del ejercicio de los derechos; otra defiende que a mayor seguridad se disfruta de menor libertad. De lo que no cabe duda es que solo en un contexto de razonable seguridad puede disfrutarse de los derechos fundamentales[3]. Pérez Royo (2010; 7)[4] señala que entre libertad y seguridad no hay tensión, porque la segunda forma parte de la primera. En ese sentido, actualmente se reconoce que la seguridad puede limitar otros derechos de forma legítima, en contraposición a visiones anteriores en las que se defendía que los derechos eran absolutos y no podían ser limitados. Son abundantes

[3] Aunque nos parece obvio y podríamos poner múltiples ejemplos para avalar esta aseveración, somos conscientes de que esta relación es compleja y presenta múltiples aristas y aspectos controvertidos.

[4] PEREZ ROYO, J. «*La democracia frente al terrorismo global*», en Terrorismo, democracia y seguridad, en perspectiva constitucional, Barcelona, 2010, págs. 7-12, pág. 7.

los ejemplos de esta limitación, pero nos ceñiremos más adelante a algunos concretos a los efectos del estudio.

Fuere como fuere, en los últimos años, las cuestiones de seguridad siempre han aparecido como elementos para justificar esas limitaciones, si bien, en las últimas décadas han surgido una serie de riesgos y amenazas que han intensificado la relevancia de la seguridad y han sido constantes en las agendas políticas a nivel mundial; también en el ámbito de la Unión Europea —ámbito que nos interesa más—. Serra Cristóbal (2016; 488)[5] cree que bajo pretextos de seguridad nacional se han defendido argumentos para la adopción de medidas que parecen más bien encaminadas a la limitación de la libertad y no tanto a garantizarla, y defiende la existencia [en la Unión Europea] de instrumentos y principios que forman parte de los fundamentos propios de esta organización política, que pueden ayudar a la adopción de políticas de lucha contra el terrorismo [y contra la delincuencia grave] que no supongan un sacrificio excesivo o desproporcionado de las libertades de los ciudadanos.

Sin ser exhaustivos, podemos citar el terrorismo internacional, la aparición de nuevos Estados fallidos, las potenciales armas de destrucción masiva o el reciente resurgimiento de las armas nucleares; o la lucha por los recursos energéticos o los movimientos migratorios derivados de situaciones de guerra, inestabilidad política o pobreza extrema, como algunos de los riesgos emergentes o amenazas que en los últimos tiempos han aparecido o vuelto, por desgracia, a las agendas nacionales [pensemos en la invasión rusa de Ucrania y cómo los elementos citados se han puesto de manifiesto]. La mayoría de los países tienen en cuenta estos riesgos a la hora de diseñar sus políticas y estrategias de seguridad nacional, y de ofrecer opciones de respuesta, pero sin que estas sean desproporcionadas en su afectación o injerencia en otros derechos. En este sentido, afirma López Aguilar (2017; 580)[6] que en un momento de la historia como el actual, «*la securitización*» ha emergido como no lo había hecho antes como prioridad política y ha impactado de forma notable en el frágil equilibrio entre libertad y seguridad.

---

[5] SERRA CRISTÓBAL, R., «*Los derechos fundamentales en la encrucijada de la lucha contra el terrorismo. Lo que el constitucionalismo y el derecho de la Unión Europea pueden ofrecer en común*», UNED, Teoría y Realidad Constitucional, núm. 38, 2016, págs. 487-503, pág. 488.

[6] LÓPEZ AGUILAR, J.F., «*La protección de datos personales en la más reciente jurisprudencia del TJUE: los derechos de la CDFUE como parámetro de validez del derecho europeo, y su impacto en la relación transatlántica UE-EE. UU.*», en UNED. Teoría y Realidad Constitucional, nº. 39, 2017, págs. 557-581, pág. 580.

Encontrar un equilibrio que satisfaga a la sociedad en este dilema *libertad vs. seguridad* surge de forma reiterada en función de acontecimientos concretos que llevan a los decisores políticos a adoptar medidas. Es el propio ciudadano quien, ante este tipo de situaciones, exige a sus gobiernos aprobar políticas hacia un mayor grado de seguridad, lo que hace que de forma reiterada surja esta tensión entre derechos. Dependiendo del momento que se considere, las posiciones mayoritarias tienden hacia un lado u otro, pero parecen inclinarse habitualmente hacia el pensamiento de que la seguridad ha sido preponderante por encima de la libertad. Lo cierto es que nunca se han vislumbrado posiciones claras en un sentido u otro. Entendemos que quizás esta falta de posición nítida es lo que hace que sea un debate inconcluso que se aborda de forma acalorada, abandonándose cuando la situación se enfría, a la espera de la siguiente oportunidad.

De forma indisoluble al derecho a la seguridad, la libertad se configura como otro de los valores de nuestras democracias y, en ese sentido, también surgen exigencias ciudadanas para que su ejercicio sea efectivo, lo que conlleva necesariamente al establecimiento de controles para hacer frente a aquellas circunstancias que puedan amenazar nuestros derechos y libertades y su ejercicio en una sociedad democrática. De forma particular, el ejercicio de las libertades se ha ido concretando a lo largo del tiempo en una serie de derechos individuales: a la intimidad, al libre movimiento, a la libertad de reunión, etcétera. La máxima expresión de estos ha dado lugar a los llamados derechos humanos y fundamentales.

En definitiva, en este pulso entre derechos, sí hay consenso en que ambos están ligados y en que las prácticas de la convivencia se han ido ajustando a lo largo de la historia, manteniendo siempre ese pulso vivo e inconformista. En esto, como en muchas otras facetas de la vida, como indica Marsal Muntalá (2005; 221)[7]: «*el análisis y valoración que podamos hacer de ellos dependen también en gran manera de nuestras visiones del mundo y nuestras posiciones políticas*». Dejaremos al margen ambas, de forma que lo que aquí se exponga y se argumente sea fruto del análisis y rigor científico.

La actual Unión Europea comenzó a formar un espacio político, en el que viven ahora más de quinientos millones de personas, con el establecimiento de un mercado único, que con el Tratado de Maastricht de 1992 pasa a configurarse también como un espacio de libertad de movimiento y circulación mediante un espacio legal armonizado.

[7] MARSAL MUNTALÁ, J., «*Seguridad versus Libertad*», disponible en http://arbor.revistas.csic.es; consultado el 15 de julio de 2022.

En ese momento, surgen derechos que son considerados como comunitarios y, entre otros, dan lugar a la creación del Espacio de Libertad, Seguridad y Justicia (ELSJ) que se desarrolla en el programa de Tampere (1999-2004) y de la Haya (2004-2009). Ya entonces se busca equilibrar el respeto de determinados derechos fundamentales y, entre otros, la seguridad respecto del intercambio de información y, de forma particular, en el respeto a la privacidad y la protección de los datos personales. Después de muchas vicisitudes, derechos recogidos en la CDFUE —en particular los artículos 7 y 8— pasan a tener el mismo valor jurídico que los Tratados y, en consecuencia, obliga también a los Estados miembros. Sin embargo, sigue estando en manos de estos [los Estados miembros] la posibilidad de adoptar medidas e iniciativas en materia de seguridad nacional, impidiendo así desplegar en toda su plenitud su protección[8].

Además, según el artículo 276 del Tratado de Funcionamiento de la Unión Europea (TFUE)[9], el TJUE no es competente para enjuiciar la proporcionalidad de las medidas adoptadas por los Estados miembros relacionadas con el orden público y la seguridad interior. Por lo tanto, a priori[10], el control de legalidad y, por añadidura, de la proporcionalidad de las medidas, deberá ser ejercido por los tribunales nacionales (Alonso, 2010; 8)[11].

A. La información como elemento imprescindible

«*Información es poder*». Esta era una frase muy repetida antiguamente entre quienes formaban parte de los servicios policiales o de

[8] Un sector de los expertos considera que el uso de esta «*cláusula habilitante*» sirve a los Estados miembros para justificar que cualquier acción en materia de seguridad debe excluir a la Unión de forma unilateral, por ser un coto reservado exclusivamente a los Estados miembros.

[9] Artículo 276 del TFUE: «*en el ejercicio de sus atribuciones respecto de las disposiciones de los capítulos IV y V del Título V de la tercer parte relativas al espacio de libertad, seguridad y justicia, el Tribunal de Justicia de la Unión Europea no será competente para comprobar la validad o proporcionalidad de operaciones efectuadas por la policía u otros servicios con funciones coercitivas de un Estado miembro, ni para pronunciarse sobre el ejercicio de las responsabilidades que incumben a los Estados miembros respecto del mantenimiento del orden público y de la salvaguardia de la seguridad interior*».

[10] Veremos más adelante que esta afirmación no es tan tajante y ofrece matices claros e importantes.

[11] ALONSO GARCÍA, R., «*Lisboa y el Tribunal de Justicia de la Unión Europea*», Papeles de Derecho Europeo e Integración Regional, Instituto de Derecho Europeo e Integración Regional (IDEIR), Universidad Complutense, nº. 1., págs. 1-30, pág. 8, en https://www.ucm.es/data/cont/docs/595-2013-11-07-lisboa%20y%20el%20derecho.pdf .

inteligencia, después también en el mundo financiero, y hoy en casi todos los ámbitos de la vida. Es cierto que cada vez hay más información de fuentes abiertas que, adecuadamente tratada, pueden aportar ventajas competitivas, bien para protegerse o para tomar decisiones que otorguen una posición de privilegio. No obstante, otro tipo de información que no es accesible al público general es igualmente importante —en ocasiones determinante— para obtener pruebas con garantías suficientes para el ejercicio posterior de la justicia, en el esclarecimiento y enjuiciamiento de delitos graves. Es en este segundo ámbito en el que nos interesa presentar la dicotomía entre seguridad y libertad.

La actividad de los servicios policiales y de inteligencia en un estado democrático está sujeta a controles. Parece una afirmación innecesaria, por obvia; no obstante, en no pocas ocasiones se cuestiona. Se establecen controles administrativos y judiciales, que garantizan una actuación adaptada a derecho y, en caso contrario, existen mecanismos de corrección y reparación del daño causado. De forma particular, respecto del objeto de nuestro estudio, nos preguntamos si un sistema «*excesivamente*» garantista, en un momento de avances tecnológicos que han eliminado las fronteras en el intercambio de información entre usuarios —aprovechado también por delincuentes— asegura la eficacia del trabajo que estos realizan en favor de la seguridad y protección de los ciudadanos y en la persecución y enjuiciamiento de los delitos graves. O, por el contrario, ¿resta eficacia a esa labor? ¿se pueden encontrar alternativas que permitan mantener la eficacia en niveles adecuados sin menoscabar los derechos y las libertades?

III. EL DERECHO A LA PRIVACIDAD Y A LA PROTECCIÓN DE LOS DATOS EN EL ÁMBITO DE LA POLICÍA Y LA JUSTICIA PENAL

Muchos autores sitúan la aparición de la protección de datos en 1890, en EE. UU., por la confluencia de varios sucesos, el más importante de ellos es la publicación del imprescindible artículo de Samuel D. Warren y Louis D. Brandeis[12], *The Right to Privacy* [El derecho a la

[12] Los autores fueron antiguos compañeros de estudios y, en el momento de la redacción del artículo, eran socios en un despacho de abogados. Era más conocido Brandeis, con reputación de uno de los mejores juristas americanos de todos los tiempos. Por su parte, Warren, que pertenecía a la alta sociedad, se molestaba porque las reuniones familiares y sociales se publicaran en la prensa sensacionalista.

intimidad], en diciembre de ese año[13], que defendía que debía concederse protección jurídica a la intimidad, partiendo de los principios consagrados en la *Common Law*. Lo ciertamente relevante del artículo fue el seguimiento masivo que de forma rápida se hizo por parte de jueces y legisladores en los EE. UU., cuando hasta ese momento solo había habido manifestaciones puntuales y fragmentadas. En Europa, en fechas muy próximas a la publicación de Brandeis y Warren, algunos autores comenzaron a teorizar también sobre los derechos de la personalidad y la necesidad de su protección jurídica (que incluía también en cierto modo la esfera privada del individuo) y no fue pacífica la doctrina en este ámbito.

Dos siglos más tarde, en el mundo actual, las sociedades dependen en gran medida del uso de las tecnologías de la información y las comunicaciones (TIC) y de la creación de productos y servicios cada vez más asequibles a los ciudadanos, que crean nuevas formas de relacionarse y comunicarse. Los datos que generan estas tecnologías y su uso nos afectan todos los días y de muchas formas diferentes, hasta el punto de que la economía mundial está basada cada vez más, al menos en algunos de sus pilares fundamentales, en el tratamiento de los datos, incluidos los personales. Estos avances han revolucionado todos los aspectos de la vida personal, familiar y profesional. Como consecuencia, también han tenido un efecto en las administraciones públicas, en los decisores políticos; o en los proveedores de servicios, que se has visto obligados a cambiar sus sistemas de gestión y procesado de la información para beneficiar a los ciudadanos, aunque también se han visto beneficiados ellos mismos. Pero, al mismo tiempo, tienen que prestar especial atención al respeto de los derechos fundamentales de los afectados, principalmente la privacidad y la protección de los datos de carácter personal.

Esta accesibilidad y capacidad de procesamiento han derivado también en la necesidad de adaptar los marcos normativos hacia la mejora en la salvaguarda de la privacidad y de la protección de los datos de carácter personal, sobre todo a aquello que pueda afectar en mayor medida a la intimidad de las personas. La Unión Europea ha regulado a lo largo de los años (con distinta intensidad) este tipo de relaciones mediante la aplicación de políticas que no siempre han sido acertadas y que han dado origen a diferentes pronunciamientos del Tribunal de Luxemburgo.

[13] NIEVES SALDAÑA, M., «*The right to privacy: la génesis de la protección de la privacidad en el sistema constitucional norteamericano, el centenario legado de Warren y Brandeis*», UNED, Revista de Derecho Político, núm. 85, 2012, págs. 195-240.

Los datos que los ciudadanos *entregan* a personas y empresas son muy variados y, en muchas ocasiones —nos atreveríamos a decir que en la mayoría de las ocasiones— sin ser conscientes de ello, lo que hace perder el control sobre la información, máxime cuando son recogidos y tratados por empresas la mayoría de las veces situadas fuera del ámbito geográfico de la Unión Europea; es decir, sometidos a movimientos internacionales con terceros países con normativas y estándares muy variados.

El derecho fundamental a la protección de los datos de carácter personal es considerado por Pérez Estrada (2019; 1300)[14] como de «*tercera generación*» e íntimamente ligado al desarrollo de las TIC; en este caso, desde el punto de vista de su incidencia negativa en el ejercicio de los derechos fundamentales. No haremos un recorrido cronológico desde los comienzos, sino que describiremos únicamente la situación actual en la UE, pues es la que el Tribunal europeo ha tenido en cuenta en la invalidación de la Directiva 2006/24/CE[15], en torno a la que gira nuestro estudio.

Desde la entrada en vigor del Tratado de Lisboa[16], la Carta tiene valor de Derecho primario[17]. Los destinatarios de esta son, en particular, las instituciones de la Unión y, por tanto, el Consejo cuando actúa en calidad de legislador, así como los Estados miembros «*únicamente cuando apliquen el Derecho de la Unión*»[18]. *Por consiguiente, su inob-*

[14] PÉREZ ESTRADA, M.J., «*La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información*», Universidad del País Vasco, 2019, en http://orcid.org/0000-0001-7402-4863, consultado el 18 de julio de 2022, págs. 1297-1330, pág. 1300.

[15] 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, en https://www.boe.es/doue/2006/105/L00054-00063.pdf .

[16] El Tratado de Lisboa, por el que se modifican el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea (DO C 306 de 17.12.2007), entró en vigor el 1 de diciembre de 2009.

[17] Vid. artículo 6.1 del Tratado de la Unión Europea (TUE), que otorga a la Carta «*el mismo valor jurídico que los Tratados*».

Véase también, European Union Agency for Fundamental Rights -FRA et al.-, 2018, pp 19-20: «*El Derecho de la UE está compuesto por Derecho primario y Derecho derivado. Los Tratados, en concreto el Tratado de la Unión Europea (TUE) y el Tratado de Funcionamiento de la Unión Europea (TFUE), han sido ratificados por todos los Estados miembros de la UE y constituyen el Derecho de la Unión Europea. Los reglamentos, directivas y decisiones de la UE han sido adoptados por las instituciones de la UE, en las que se ha delegado tal autoridad en virtud de los Tratados, y constituyen el Derecho derivado de la UE*».

[18] Artículo 51.1 de la Carta.

servancia por parte del legislador de la Unión puede llevar a la anulación por el Tribunal de Justicia del acto de que se trate.

El artículo 8.1 de la Carta dispone que «toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan»[19]*. Según el Tribunal de Justicia, «este derecho fundamental se halla íntimamente ligado al respeto a la vida privada, consagrado en el artículo 7»*[20] de la Carta, según el cual «*toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones*».

El derecho al respeto de la vida privada se recoge también en el artículo 8.1 del Convenio Europeo de Derechos Humanos (CEDH) y, en consecuencia, con arreglo al artículo 52.3 de la Carta tiene el mismo sentido y alcance que el que le otorga el CEDH[21].

Los datos personales[22] solo pueden ser objeto de tratamiento[23] si se respetan determinados principios comunes en dicho ámbito: los principios de lealtad, finalidad, legitimación, transparencia y control por autoridades independientes; y sólo pueden limitarse si se respetan determinadas condiciones[24] y las justificaciones de la injerencia

[19] Este derecho se repite en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea (TFUE) entre las disposiciones de aplicación general.

[20] Punto 47 de la sentencia del 9 de noviembre de 2010, Volker, C-92/09 y C-93/09.

[21] Para una descripción de las condiciones de aplicación del artículo 8 del CEDH, y en particular de las condiciones en que puede justificarse una injerencia en el derecho al respeto de la vida privada, véase dictamen del Servicio Jurídico de 20 de junio de 2001 (doc. 10146/01, de la Secretaría General del Consejo).

[22] Constituyen datos de carácter personal «*toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona*». Art. 4.1) del Reglamento General de Protección de Datos de la UE.

[23] Constituye un tratamiento «*cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción*». Art. 4.2) del Reglamento General de Protección de Datos de la UE.

[24] El artículo 8.2 del CEDH sólo admite una injerencia «*en tanto en cuanto […] esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de los derechos y las libertades de los demás*» Por su parte, el artículo 52.1 de la Carta sólo admite una limitación: que esté establecida «*por la ley y [respete] el contenido esencial de dichos derechos […] dentro del respeto del principio de proporcionalidad, sólo podrán introducirse limitaciones cuando*

exigen *una interpretación estrecha*[25]. Son estas disposiciones las que sirven de marco de análisis al TJUE, que en este ámbito sigue al Tribunal Europeo de Derechos Humanos (TEDH) para examinar la compatibilidad de una medida de tratamiento de datos con los derechos en cuestión[26]. En consecuencia, las medidas previstas en la normativa europea deberán ser analizadas en función de estos criterios.

IV. LA IMPORTANCIA DE LOS METADATOS DE LAS COMUNICACIONES ELECTRÓNICAS A EFECTOS DE LA APLICACIÓN DE LA LEY

El Convenio nº. 108 del Consejo de Europa estableció que por datos de carácter personal había de entenderse «*cualquier información relativa a una persona física identificada e identificable*», que llamó «*persona concernida*»[27]. Este convenio, actualizado en 2018, varía solo ligeramente la definición, pero sí cambia la denominación de la persona concernida, a la que ahora llama «*titular de datos o interesado*». Por su parte, la Directiva 95/46/CE[28] recogió que por «*datos personales*» se entendía «*toda información sobre una persona física identificada o identificable*», que en su caso denomina de forma diferente al Convenio, como «*interesado*». La más reciente norma de la Unión Europea en la materia, el Reglamento General de Protección de Datos[29], se refiere al titular de los datos como «*el interesado*». El TJUE también se ha pronunciado sobre el concepto de dato personal, reconociendo que es muy amplio.

---

sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás».

[25] Sentencia del TEDH, Rotaru, 4 de mayo de 2000, nº 2841/95, 47.

[26] Vid. Sentencia Volker antes citada. Véase también las sentencias de 20 de mayo de 2003, Österreichischer Rundfunk, C-465/00, C-138/01 y C-139/01, Rec. 2003 p. I-4989.

[27] Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981, art. 2, en https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447.

[28] Directiva 95/46/CE del Parlamento 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, en https://www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678 .

[29] Reglamento (UE) 2016/679 del Parlamento y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) en https://www.boe.es/doue/2016/119/L00001-00088.pdf .

Un tipo particular de datos: los datos de tráfico y de localización que rodean a las comunicaciones electrónicas —que hemos englobado bajo el concepto genérico de metadato, puesto que no incluyen información de contenido de las comunicaciones—, no son *inofensivos*; todo lo contrario, aportan una información que puede generar peligros evidentes a la hora de recopilarlos, almacenarlos, tratarlos y transmitirlos, provocando consecuencias sobre determinados derechos de sus titulares. Pueden aportar información sobre quiénes han estado en contacto de diferentes maneras —mensajes, correos electrónicos, llamadas, etcétera—, en qué momento y de qué forma; que adecuadamente tratados, pueden revelar hábitos y comportamientos precisos de la vida cotidiana de las personas, incluso de aquellos que puedan ser especialmente sensibles; o relaciones entre personas o la pertenencia a un grupo determinado; o movimientos precisos, etcétera. Como revela Fernández Rodríguez (2016; 96)[30], pueden incluso incidir en la libertad de expresión de las personas, en la medida en que «*un individuo que sabe que se recaban esos datos puede autocensurarse a la hora de efectuar una comunicación o de establecer ciertas iniciativas públicas*».

La Directiva 2002/58/CE sobre privacidad electrónica[31] regula este tipo de comunicaciones entre los europeos. Aunque está en proceso de actualización, a través de un reglamento europeo que se encuentra todavía en discusión en las instituciones europeas, sigue en vigor[32]. Establece normas estrictas para garantizar un alto nivel de protección de los datos de las comunicaciones electrónicas, pero permite a los Estados miembros fijar restricciones y limitaciones y adoptar medidas que prevean la conservación de datos por un determinado límite temporal.

Dentro de esas posibilidades es donde se enmarca la aprobación de la Directiva 2006/24/CE de conservación de datos, que establecía normas específicas para armonizar las medidas adoptadas por todos

[30] FERNÁNDEZ RODRÍGUEZ, J.J., «*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, Centro de Estudios Políticos y Constitucionales, págs. 93-122, pág. 96.

[31] 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 https://www.boe.es/doue/2002/201/L00037-00047.pdf .

[32] En 2017, la Comisión Europea presentó un borrador de Reglamento sobre privacidad y las comunicaciones electrónicas que sigue, a la fecha de elaboración del presente estudio, en discusión en el correspondiente grupo de trabajo del Consejo de la Unión Europea.

los Estados miembros de la Unión. Empero, fue invalidada *ex tunc*[33] por el TJUE en 2014. A esta sentencia siguieron otras [que veremos con detalle] que han configurado una situación compleja con implicaciones directas para las capacidades operativas de los servicios policiales y de las autoridades judiciales que todavía hoy no se han podido valorar en toda su extensión.

Una cuestión relevante que requiere de análisis es la que, de forma muy pertinente, plantea Fernández Rodríguez (2016; 102)[34], acerca de si es necesario conservar «los datos de tráfico [y de localización] por razones de seguridad».

Como hemos señalado antes, los ciudadanos realizan cada vez más actividades y transacciones cotidianas utilizando redes y servicios de comunicaciones electrónicas, y todos y cada uno de los movimientos a través de estas redes generan una serie de datos que permiten a los proveedores de servicios de comunicaciones electrónicas cumplir con una serie de funciones administrativas y comerciales[35]. Otro tipo de datos, los datos de los abonados[36] [en ocasiones, de los usuarios], también son tratados a efectos de gestión de las suscripciones y conservados por estos durante un determinado un tiempo, debiendo suprimirlos (o *enmascararlos*[37]) cuando ya no sean necesarios a los fines previstos. En consecuencia, se genera y se trata un volumen ingente de información de prácticamente toda la población. No se cuestiona

[33] Es decir, desde la fecha en que entró en vigor, en 2006.

[34] FERNÁNDEZ RODRÍGUEZ, J.J., «*Los datos de tráfico de comunicaciones…*» *op. cit.* pág. 102.

[35] El artículo 2 de la Directiva 2002/58/CE, sobre privacidad y las comunicaciones electrónicas distingue «*tres categorías de datos principales generados durante una comunicación:*

— Los datos que constituyen el contenido de los mensajes enviados durante la comunicación y que son estrictamente confidenciales;

— Los datos necesarios para establecer y mantener la comunicación -los llamados metadatos, que en la Directiva reciben el nombre de «datos de tráfico»-, como la información relativa a las partes de la comunicación, la hora y la duración de la comunicación;

Los metadatos contienen datos específicamente relacionados con la localización del dispositivo de comunicación, los denominados «datos de localización», que son al mismo tiempo datos sobre la localización de los usuarios de los dispositivos de comunicación, especialmente en lo que respecta a los usuarios de dispositivos de comunicaciones móviles»(Directiva europea sobre privacidad electrónica, 2002; L 201/434).

[36] Datos que se aportan a la hora de contratar un servicio con un proveedor de servicios, como el nombre, dirección de facturación, cuenta bancaria, NIF, etcétera.

[37] Abordaremos, siquiera de forma superficial, las técnicas de *anonimización* y *seudoanonimización* como alternativas hacia el aumento de la seguridad en los datos conservados por los operadores de telecomunicaciones.

que las empresas del sector necesitan esos datos para poder prestar el servicio, cobrarlo y reaccionar ante errores, quejas o sugerencias.

Más allá de los fines comerciales, también pueden invocarse fines de *seguridad u orden público*[38] para justificar el tratamiento ulterior. No cabe duda de que su disponibilidad puede ser importante para determinados fines policiales y judiciales, como la investigación, persecución y enjuiciamiento de conductas delictivas graves. Algunos expertos policiales han comparado los metadatos con las huellas dactilares: «*mientras que en el mundo físico se pueden recoger huellas físicas, en el mundo digital los datos de tráfico y de localización son el equivalente digital a las huellas digitales*»[39].

Por ello, las autoridades de los Estados miembros podían, si era necesario y acorde con la legislación aplicable a nivel nacional, solicitar el acceso a los datos de localización y tráfico almacenados por los operadores para sus fines empresariales, así como exigir su almacenamiento posterior a partir de la fecha de solicitud.

Sin embargo, con los cambios en los modelos de negocio y las ofertas de nuevos servicios[40], los operadores dejaron de guardar determinados datos que ya no eran necesarios para su labor de gestión interna y que suponía costes adicionales, lo que dificultaba las labores de aplicación de la ley y, al mismo tiempo, servía a los intereses de los delincuentes. La Directiva 2006/24/CE venía a hacer frente a la pérdida de forma lenta, pero segura, de uno de los instrumentos más importantes para prevenir y combatir la delincuencia grave y el terrorismo, ante la disparidad de normas nacionales y quizás también presionada por los atentados de Madrid y de Londres y la solicitud de soluciones de los jefes de estado y de gobierno en las reuniones del Consejo Europeo[41], que manifestaron que la lucha contra el te-

[38] Los fines de *orden público* se entienden en el presente documento como referidos a los intereses de orden público mencionados en el artículo 15 de la Directiva 2002/58: «*la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, la prevención, la detección y el enjuiciamiento de delitos o del uso no autorizado del sistema de comunicaciones electrónicas. A efectos de este documento, se entiende que los fines policiales se limitan a la prevención, investigación, detección y persecución de delitos*».

[39] «*En el caso de un delito cometido total o parcialmente en el mundo electrónico, si no hay de tráfico [de datos], no puede haber investigación. Así de sencillo*». Declaración de John Abbott, C.B.E, QPM. B.A. (Hons), antiguo director general del Servicio Nacional de Inteligencia Criminal, Reino Unido, en la primera sesión plenaria del Foro de la Unión Europea sobre Ciberdelincuencia.

[40] Como tarifas planas, servicios de prepago o incluso gratuitos, que se vio reforzada con la aparición de la voz sobre IP.

[41] En la lucha contra la delincuencia grave y organizada se pueden usar los mismos argumentos que justifican la necesidad de garantizar el derecho a la seguridad

rrorismo era un objetivo de interés general contra el que no se puede actuar de forma individual (el interés general también ha sido reconocido por el TJUE)[42]. La consecuencia lógica es la inexorable *tensión* entre derechos y la búsqueda de equilibrio entre los intereses en juego. Como indica el filósofo Zygmunt Bauman: «*nadie ha encontrado todavía en la historia y en el planeta la fórmula de oro para la mezcla perfecta de seguridad y libertad*»[43].

V. EL TJUE COMO GARANTE DE LOS DERECHOS DE LOS EUROPEOS

Al TJUE le corresponde la potestad jurisdiccional en la Unión Europea, según recoge el artículo 19.1 del TUE, lo que le confiere legitimidad en la interpretación y aplicación del derecho comunitario y en la armonización de las normas en ámbitos compartidos con los Estados miembros, como son las materias de derecho penal. En su labor diaria, es fundamental el mecanismo previsto en el artículo 267 del TFUE, que regula la cuestión prejudicial. Esta permite al juez de un Estado miembro someter a su criterio aquellos casos en los que tenga dudas sobre la interpretación del Derecho comunitario o sobre su validez a los efectos del proceso que está sustanciando. Sin embargo, aunque la facultad para recurrir a la cuestión prejudicial corresponde al juez [es potestativo, salvo para cuestiones sobre asuntos pendientes ante un órgano jurisdiccional nacional cuyas decisiones no den lugar a la posibilidad de recurso posterior en el Derecho interno], las partes en el proceso también están habilitadas para proponer a este la presentación de tal medida, o hacerlo el propio Tribunal de oficio[44]. Si se cuestiona la validez de una norma europea, este [el juez o tribunal] deberá presentar necesariamente la cuestión prejudicial, ya que sólo el TJUE tiene competencia para juzgar la validez de estas normas; debiendo pararse el proceso principal que ha suscitado la consulta has-

de los ciudadanos en una sociedad democrática y de libre convivencia, según recoge el artículo 6 de la Carta de Derechos Fundamentales de la Unión Europea.

[42] Como ejemplo, vid. Sentencia del TJUE en el *Caso Yasin Adbullah Kadi y Barakaat International Foundation* vs. Consejo de la Unión Europea y Comisión de las Comunidades Europeas, de 3 de septiembre de 2008, apartado 363; y Sentencia en el *Caso Stichting Al-Aqsa* vs. Consejo de la Unión Europea y Reino de los Países Bajos contra Stichting Al-Aqsa, de fecha 15 de noviembre de 2012, apartado 130.

[43] Vid. diálogo entre Fernando Schüler y Mario Mazzilli, en https://www.youtube.com/watch?v=in4u3zWwxOM, visionado el 10 de mayo de 2021.

[44] Existen casos particulares y excepciones a esta regla general, pero a los efectos de este estudio, en el que no cuestionamos la competencia del TJUE para conocer de los casos planteados sobre la validez de la Directiva 2006/24/CE, solo reseñaremos la especificidad de cómo se insta su pronunciamiento sobre la norma europea.

ta su resolución; que afectará no solo al Estado miembro recurrente sino también al resto de miembros, en la medida en que conozcan de un supuesto idéntico.

Sobre los efectos de las sentencias, en el supuesto de declarar la invalidez de una norma europea, estos se extenderán *ex tunc*, si bien el Tribunal podrá modular o limitar la aplicación retroactiva, basándose en motivos de seguridad jurídica.

El TJUE es competente también para conocer de las violaciones a los derechos fundamentales amparados por la Carta. Para ello, tanto los Estados miembros como las instituciones europeas, pero también de los ciudadanos, podrán recurrir a la jurisdicción correspondiente, y serán los jueces y tribunales de estas quienes insten al Tribunal europeo a pronunciarse, si albergan dudas respecto de la potencial lesión de los derechos de los particulares.

A medida que la Unión Europea ha ido avanzando en integración, se ha producido también un mayor impacto de la normativa comunitaria en la vida los ciudadanos y, de forma lógica, también sobre el ejercicio de los derechos fundamentales que les asisten. Uno de los ámbitos en los que se ha observado esta influencia [quizás de las más acusadas] es el correspondiente a la investigación, persecución y enjuiciamiento de los delitos. De forma paralela, se han reforzado las competencias del Tribunal europeo y se ha mejorado la forma jurídica de la Carta[45]. En definitiva, se ha reforzado el papel del TJUE como garante de los derechos. Mantiene Fernández Ogallar (2014; 124)[46] que los Estados miembros han sido siempre cuidadosos a la hora de decidir qué asuntos someten a consideración del Tribunal y, entre ellos, se encuentran los que afectan a materias de derecho penal, propiciando así avances más tortuosos y lentos[47].

Antes del Tratado de Lisboa, el Tribunal europeo recurría de forma frecuente a las sentencias del TEDH, hasta el punto en que se convirtió en su principal fuente de *inspiración*. A partir de ese momento, tiende más al uso de un criterio propio y ejerce un mayor control de la legalidad de cualquier intromisión en los derechos fundamentales. En este proceso de emancipación, según algunos autores, ha alcan-

[45] En el Tratado de Lisboa.

[46] FERNÁNDEZ OGALLAR, N., *El derecho penal armonizado en la Unión Europea*, Madrid, Dykinson, 2104.

[47] Estas materias afectan fundamentalmente al Tercer pilar y, aunque el Tratado de Lisboa elimina esa estructura de tres puntos de apoyo, que propicia la extensión de las competencias del Alto Tribunal al derecho penal (entre otros ámbitos) y, en consecuencia, también a su capacidad de actuación sin la previa aceptación de los Estados miembros.

zado el papel de un tribunal constitucional europeo con la CDFUE como punto de referencia[48].

VI. CONTEXTO LEGAL Y POLÍTICO SOBRE LA CONSERVACIÓN DE METADATOS. DEL *CASO DIGITAL RIGHTS IRELAND*[49] *HASTA HOY*

Para las autoridades encargadas de la aplicación de la ley, el valor de los datos de tráfico y de localización de las comunicaciones electrónicas radica no solo en su potencial para establecer vínculos entre sospechosos y fijar patrones de comunicación entre diferentes personas, sino también como ayuda (en algunos casos determinante) en la localización de víctimas de delitos graves y para la obtención de pruebas sobre el escenario de un crimen o incluso para descartar la participación de posibles sospechosos.

En un primer momento, el Consejo de la UE propuso un proyecto de decisión marco sobre esta misma materia sobre la base de los poderes de cooperación policial de la Unión, que recogía la misma obligación de conservación de metadatos que la que después se incluyó en la directiva. Sin embargo, la oposición o reticencias del Parlamento Europeo y de las autoridades en materia de protección de datos, precisamente porque adolecía de falta de proporcionalidad, hicieron que se retirara la propuesta. En 2005, la Comisión presentó una propuesta de directiva[50] que introducía una obligación general de conservar ciertas categorías de datos procedentes de todos los usuarios, con el propósito de la lucha contra el delito grave, según fuera definido por cada Estado miembro en su normativa nacional[51]. Obli-

---

[48] RIZZO, G., *Derecho a la privacidad y seguridad en el espacio público europeo*, tesis doctoral, Universidad Carlos III de Madrid, 2019, pág. 286, en http://dialnet.unirioja.es/servlet/tesis?codigo=267383, consultado el 12 de agosto de 2022.

[49] Sentencia del Tribunal de Justicia (Gran Sala) de 8 de abril de 2014, en los asuntos C-293/12 y C-594/12.

[50] Propuesta de la Comisión para una Directiva del Parlamento Europeo y del Consejo sobre la retención de información procesada en relación con la provisión de los servicios de comunicación electrónica pública y por la que se modifica la Directiva 2002/58/EC, COM (2005) 438 final, 21 de septiembre de 2005.

[h]ttp://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2005/0438/COM_COM(2005)0438_EN.pdf, consultada el 02.05.21.

[51] En el artículo 1, relativo al objeto, se proponía: «*armonizar las disposiciones de los Estados miembros relativas a las obligaciones de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones en relación con la conservación de determinados datos generados o tratados por los mismos, para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación na-*

gaba a los proveedores de servicios a retener la información por un período entre seis y veinticuatro meses, en aras a asegurar que esta estuviera disponible para la investigación, detección y persecución del delito grave. Los proveedores fueron obligados también a poner esa información a disposición de las agencias encargadas de hacer cumplir la ley, en caso de ser solicitada. Sin embargo, no se especificaba cómo se accedería a la información ni cómo sería usada por las autoridades competentes. Con esa obligación, los proveedores de servicios intervenían/interferían sobre los derechos de los ciudadanos en cumplimiento de una obligación legal impuesta por la norma europea. Además, se les obligaba a establecer una serie de medidas que permitieran garantizar la seguridad de los datos conservados[52].

A partir de ese momento, los Estados miembros reformaron sus legislaciones domésticas en la materia, en base a una norma que les habilita a adoptar medidas legales para establecer excepciones a los derechos contenidos en la misma por razones de protección de la seguridad nacional, la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos. El devenir posterior ya lo hemos anunciado[53]: el TJUE dictaminó que la conservación de datos constituye en sí misma una excepción al deber de garantizar la confidencialidad de las comunicaciones realizadas a través de una red pública de comunicaciones electrónicas disponibles al público que debe ser interpretada de un modo altamente restrictivo y que una conservación de todos los datos personales de todos los usuarios, durante un periodo de tiempo tan amplio y en relación con todos los medios de comunicación electrónica, sin diferenciación, limitación o excepción en función del objetivo que se pretende lograr, no era admisible. Aventuraba con acierto Ortiz-Pradillo (2020; 6)[54] que tras

cional de cada Estado miembro». Se aplicaba «*a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado. No se aplicará al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas*» (Directiva 2006/24/CE, 2006; L 105/56).

[52] El artículo 7 de la Directiva 2006/24/CE obligaba a los proveedores de servicios a implementar «*medidas técnicas y organizativas adecuadas para protegerlos de la destrucción accidental o ilícita, pérdida accidental o alteración, así como almacenamiento, tratamiento, acceso o divulgación no autorizados o ilícitos*».

[53] En 2009 el TJUE desestimó ya otro recurso planteado también por Irlanda respecto de la base jurídica de la Directiva de Conservación de Datos. El TJUE lo desestimó, aunque en el fundamento 57 de su Sentencia puso en duda la legalidad de la Directiva. Ver Sentencia TJUE (Gran Sala), Irlanda contra el Parlamento Europeo y el Consejo de la Unión Europea, asunto C-301/06, de 10 de febrero de 2009.

[54] ORTIZ-PRADILLO, J.C., «*Europa: auge y caída de las investigaciones penales basadas en la conservación de datos de comunicaciones electrónicas*», en Revista General de Derecho Procesal, núm. 52 (2020), págs. 1-28, pág. 6.

las sentencias del TJUE, la adopción de criterios concretos[55] para el establecimiento de un sistema de conservación de datos con carácter compatible con la Carta se vislumbra muy complicado, no tanto para el acceso a los datos como para la conservación, lo que supondrá una tarea difícil para el legislador.

Quizás uno de los *pecados originales* fue la base jurídica escogida sobre la que se apoyó la directiva, relacionada con la armonización del Mercado Interior[56]. Este fue uno de los motivos que llevó a Irlanda a presentar una cuestión prejudicial, al considerar que en realidad la directiva pretendía facilitar la investigación, detección y enjuiciamiento de infracciones penales y, en consecuencia, no era la base jurídica adecuada. En este punto de la historia, el Tribunal europeo no avaló la postura irlandesa por cuanto consideró que los preceptos de la directiva se limitaban «*a las actividades de los prestadores de servicios y no regulaba el acceso a los datos ni la explotación por las autoridades policiales o judiciales de los Estados miembros*»[57], dejando esta última parte a los Estados miembros, por corresponder al ámbito penal.

Sin embargo, en los apartados 39 y 40 de la *Sentencia Digital Rights Ireland* dictaminó que no se había producido vulneración del contenido esencial de los derechos previstos en los artículos 7 y 8 de la Carta[58], ya que no se accedía al contenido de las comunicaciones, pero tenían que aplicar las normas de protección de los datos personales. Por lo tanto, no excluía la posibilidad de establecer un régimen europeo de conservación de datos, lo que supuso una ventana de oportunidad que, eso sí, llevaba a la necesidad de buscar opciones y diseñar ese nuevo sistema, teniendo en cuenta el resto de la doctrina que también fija esta sentencia y las que vinieron más tarde[59].

---

[55] Veremos más adelante cada uno de esos criterios y su análisis concreto.

[56] Materia del Primer pilar y no relacionada directamente con el ámbito de la cooperación policial y judicial, que corresponde al Tercer pilar.

[57] Sentencia TJUE, de 10 de febrero de 2009, Irlanda/Parlamento Europeo y Consejo de la UE, C-301/06, Rec. P. I-00593, apartado 80.

[58] Algunos autores consideran que esta decisión del TJUE es polémica, ya que la distinción entre el contenido del mensaje y los metadatos se torna difusa de cara a la protección del derecho a la privacidad, si se tiene en cuenta que la tecnología de vigilancia actual es lo suficientemente invasiva incluso sin acceso al contenido de las comunicaciones. Véase PUERTO, M.I y SFERRAZZA TAIBI, P., «*La sentencia Schrems del Tribunal de Justicia de la Unión Europea: un paso firme en la defensa del derecho a la privacidad en el contexto de la vigilancia masiva transnacional*», en Revista Derecho del Estado, núm. 40, enero-junio de 2018, págs. 209-236, pág. 227.

[59] Como punto llamativo y novedoso en las sentencias del TJUE, en este caso, considera que la injerencia en los derechos fundamentales afectados es «*especialmente grave*».

La pregunta que nos surge a continuación es *¿qué ocurre con las legislaciones nacionales de transposición de la directiva una vez que el TJUE la declaró inválida?*

A. Segunda sentencia. El TJUE confirma su doctrina

A raíz de la decisión del *Caso Digital Rights Ireland*, un proveedor sueco de comunicaciones electrónicas llamado Tele2 dejó de retener datos y notificó a la autoridad sueca de control de las telecomunicaciones que, además, suprimiría los datos conservados hasta ese momento, al considerar que la legislación nacional sueca no cumplía con las normas establecidas por el Tribunal europeo. El Tribunal de Apelación sueco que entendió del caso suspendió el procedimiento iniciado y planteó una cuestión prejudicial.

Al mismo tiempo, en el Reino Unido se puso en duda la legalidad de la Ley de Retención de Datos y Poderes de Investigación de 2014 (DRIPA), que se había promulgado después de la sentencia de *Caso Digital Rights Ireland*. En este caso, la nueva ley británica pretendía mantener el sistema de conservación presentándolo como medida nacional. El Tribunal de Apelación planteó también una cuestión prejudicial.

En 2016, en la sentencia del *Caso Tele2 Sverige*[60], el Tribunal confirmó que el artículo 15, apartado 1[61], de la Directiva de privacidad electrónica impide que la legislación nacional pueda prescribir una conservación de datos generalizada e indiscriminada, pero también que esta no impide que la legislación nacional pueda imponer una

[60] Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) «Tele 2 and Watson», de 21 de diciembre de 2016, Casos C-203/15 y C-698/15.

[61] El TJUE se centra en la cuestión de si el artículo 15, apartado 1, de la directiva 2002/58/CE, teniendo en cuenta los artículos 7, 8 y 52.1 de la Carta «*… debe interpretarse en el sentido de que se opone a una legislación nacional[…] para la conservación general e indiscriminada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados con respecto a todos los medios de comunicación electrónica*». La sentencia enmarca los espacios de las excepciones del artículo 15, apartado 1, al exigir que estas se consideren de manera excepcional, de forma que los Estados no puedan esgrimir, según indica en el apartado 91, razones especiales relacionadas con la seguridad pública para restringir de una forma razonable la protección de los derechos fundamentales recogidos en la Carta y, en consecuencia, la normativa nacional debe prever que la excepción al principio de confidencialidad debe guardar relación con la gravedad de la intromisión en los derechos fundamentales que representa el acceso, por lo que la justificación estará en la lucha contra el terrorismo y la delincuencia grave (apartado 115). El Tribunal considera también que la excepción prevista en el apartado 1 del artículo 15 «*debe interpretarse estrictamente*».

«*conservación selectiva a los efectos de la lucha contra el delito grave, a condición de que esté limitada a lo estrictamente necesario*». Este pronunciamiento mantuvo las esperanzas de quienes estaban analizando la situación desde 2014 para ver cómo cumplir con los requerimientos derivados de la primera sentencia y no «tirar por tierra» el trabajo pasado, presente y futuro de los cuerpos policiales y los sumarios todavía en fase de instrucción en los juzgados y tribunales. El optimismo no duró demasiado, ya que, en definitiva, con algunos matices, confirmó su doctrina anterior.

El TJUE fijó también en esta ocasión las salvaguardas que han de recoger las normativas nacionales: *i) la conservación de los datos sin contenido debe ser la excepción; ii) el propósito de la conservación debe ser restringido a la lucha contra el delito grave; iii) debe ser limitada a lo estrictamente necesario; iv) el acceso a la información retenida debe ser objeto de revisión previa por un tribunal o autoridad independiente; v) la información debe ser conservada solo dentro de la Unión Europea*.

Esta sentencia se diferencia fundamentalmente de la anterior por el hecho de que lo que se cuestiona no es una directiva europea, sino la legislación nacional de uno de sus Estados miembros, por lo que, de forma lógica, impactaba directamente en la actuación nacional a partir de ese momento. Y así fue, pues a principios de 2017, las instituciones europeas tomaron conciencia de la gravedad de la situación y constituyeron un grupo de trabajo para analizar la situación y buscar vías de solución. En realidad, en esta sentencia se dilucida la capacidad de los parlamentos nacionales para adoptar normas de conservación de datos, en transposición de una norma europea, que les permita actuar de forma eficiente en la lucha contra el terrorismo y la delincuencia grave y, al mismo tiempo, que estas sean respetuosas con los derechos fundamentales de los afectados.

El TJUE examina un segundo punto relevante: si es compatible con la Carta «*… el acceso […]a los datos conservados [de personas distintas a los investigados], cuando dicha legislación no restringe el acceso únicamente al objetivo de luchar contra la delincuencia grave, […]*» y se pronuncia en el sentido de que solo podrá preverse para casos de delitos graves, salvo en «*situaciones particulares*», como las que tienen que ver con la seguridad nacional, la defensa o la seguridad pública, en las que podría concederse el acceso a los datos de otras personas cuando «*existan elementos objetivos que permitan considerar que esos datos podrían, en un caso concreto, contribuir de modo efectivo a la lucha contra dichas actividades*» (apartado 119).

Esto hace que el juez (o la autoridad legal con capacidad para autorizar la medida[62]) que autoriza el acceso a los datos, en su resolución motivada debe realizar un juicio de proporcionalidad entre la gravedad de la injerencia en los derechos fundamentales y la gravedad de los hechos delictivos, de forma que solo en los casos de delitos graves se debería admitir el acceso a datos electrónicos de carácter personal que supongan una intromisión grave en los derechos a la privacidad y a la protección de los datos personales.

Respecto del concepto de gravedad del delito, nos surge la pregunta de *¿cómo podemos establecer o hemos de considerar que un delito es grave?* La sentencia que veremos a continuación aporta elementos interesantes precisamente respecto de esta cuestión.

B. Caso C-207/16 Ministerio Fiscal

La condición relativa a la gravedad del delito fue posteriormente especificada en el *Caso C-207/16 Ministerio Fiscal*[63], que se refiere al acceso a los datos conservados y no a la conservación en sí misma. El Tribunal estableció que «*si el acceso a determinados tipos de metadatos no representa una interferencia grave en los derechos fundamentales de privacidad y protección de los datos personales, las agencias encargadas de la aplicación de la ley podrán acceder a ellos para la investigación y persecución de delitos no graves*».

La cuestión prejudicial fue planteada por un juzgado de Tarragona, lo que a la luz de la sentencia del *Caso Tele2 Sverige*, teniendo en cuenta que se preguntaba explícitamente por el modo de proceder de acuerdo con la legislación española, podría haber dado lugar a que el régimen español de conservación de datos fuera declarado contrario al Derecho de la UE, como ocurrió respecto del planteamiento de la empresa sueca. Sin embargo, el Tribunal interpretó el alcance de la cuestión de forma diferente. Básicamente, redujo la cuestión a aspectos de acceso a los datos y no valoró el sistema español de conservación. Podemos interpretar un cambio de criterio del Tribunal, ante una interpretación excesivamente estricta en el caso sueco. Ahora, el acceso a los datos retenidos puede concederse incluso en los casos en los que no se investigan «*delitos graves*», siempre que se tenga en consideración la proporcionalidad de la medida, de forma que el cri-

[62] Aunque en España solo la autoridad judicial puede autorizar estas acciones, en otros Estados miembros se asigna a determinada autoridad administrativa independiente.

[63] Sentencia TJUE Caso C-207/16 Ministerio Fiscal, 2 de octubre de 2018.

terio de gravedad del delito queda matizado o ponderado mediante la valoración de la medida de acceso a los datos en función de su mayor o menor interferencia en los derechos fundamentales en juego[64].

C. Nuevos pronunciamientos a cuestiones prejudiciales planteadas

1. Sentencia de octubre de 2020

Posteriormente, se presentaron otras peticiones de decisión prejudicial por el Tribunal de Competencias de Investigación del Reino Unido (*Investigatory Powers Tribunal*)[65], el Tribunal Constitucional de Bélgica[66], el Consejo de Estado (*Conseil d'État*) de Francia[67] y el Tribunal Supremo de Estonia[68].

En su sentencia de 6 de octubre del pasado año (Casos acumulados C-511/18, C-512/18 «*La Quadrature de Net et al./Ordre des barreaux francophones et germanophone et al.*») el Tribunal confirmó una vez más su doctrina anterior en el sentido de que los datos de las comunicaciones electrónicas son confidenciales y, de forma general [sin restricción alguna], no pueden conservarse de manera generalizada e indiferenciada. En este caso, establece excepciones limitadas a este

[64] El Abogado General Campos Sánchez-Bordona, en sus conclusiones 66 y 67 del caso defiende que no se han producido cambios en el parecer del Tribunal y que no se autoriza en ningún caso un régimen nacional de conservación masiva e indiscriminada de datos personales, de modo que no hay modificación respecto de su doctrina expresada en la Sentencia del Caso Tele2 Sverige y Watson.

[65] Asunto C-623/17. La petición de decisión prejudicial se refiere al ámbito de aplicación del Derecho de la Unión en relación con medidas adoptadas a nivel nacional con el fin de proteger la seguridad nacional.

[66] Asunto C-520/18. En esta petición de decisión prejudicial, el Tribunal Constitucional belga pregunta si estaría o no justificado un sistema de conservación general de datos que i) persiga una finalidad más amplia que la lucha contra la delincuencia grave (a saber: combatir otras formas de delincuencia o garantizar la seguridad nacional y la defensa del territorio) o ii) tenga por objeto dar cumplimiento de las obligaciones positivas establecidas en los artículos 4 y8 de la Carga (prohibición de la tortura y protección de los datos personales).

[67] Asunto C-511/18. Una de las peticiones de decisión prejudicial del Conseil d'État francés se refiere al marco jurídico de la conservación de datos para las investigaciones penales, y en ella el Conseil d'État plantea una cuestión similar a la del Tribunal Constitucional belga, a saber, si una conservación general de datos puede justificarse en virtud del derecho a la seguridad. El asunto C-512/18 se refiere al marco jurídico de la conservación de datos para los servicios de inteligencia. Al igual que en el caso del Reino Unido (asunto C-623/17), el Conseil d'État plantea al Tribunal de Justicia si el régimen de conservación de datos está justificado dada la amenaza terrorista existente.

[68] Asunto C-746/18 relativo al acceso a datos conservados.

principio en relación con la seguridad nacional, la defensa y la seguridad pública; o la prevención, investigación, descubrimiento y persecución de delitos; que hacen que, de nuevo, se despierte optimismo e interés en los expertos que estaban analizando el problema desde hacía ya varios [demasiados] años. La sentencia recoge los supuestos y situaciones en los que esta puede tener cabida. Nos centraremos en aquello que se «*permite*», pues es ahí donde se deberán buscar las posibles soluciones que equilibren los intereses enfrentados:

En los apartados 134 y siguientes, reconoce que el artículo 4, apartado 2, del TUE establece que la seguridad nacional sigue siendo responsabilidad exclusiva de cada Estado miembro y les corresponde, entre otras cuestiones, la prevención y el castigo de actividades capaces de desestabilizar gravemente las estructuras constitucionales, políticas, económicas o sociales fundamentales de un país y, en particular, de amenazar directamente a la sociedad, a la población o al propio Estado, como las actividades terroristas (apartado 135). Por tanto, en situaciones reales, presentes y previsibles no se opone a que se recurra a la emisión de órdenes para […] que se retengan, de forma general e indiscriminada, los datos […] de todos los usuarios […] durante un período de tiempo limitado (apartado 137), exigiendo salvaguardas estrictas ante riesgo de abuso y que la conservación, aunque renovable, no sea sistemática (apartado 138), además de sometida a revisión por un tribunal u organismo administrativo independiente (apartado 139).

En los apartados 140 y siguientes, dictamina que el Derecho de la UE no se opone a la conservación selectiva de datos de tráfico y de localización de grupos de personas o bajo criterios geográficos, establecidos de forma objetiva y no discriminatoria, con el fin de salvaguardar la seguridad nacional, luchar contra la delincuencia grave y prevenir las amenazas graves para la seguridad pública, siempre que el período se limite a lo estrictamente necesario. A pesar de ello, no pueden conservarse de forma sistemática y continua (apartado 142).

En los apartados 152 y siguientes, recoge la posibilidad de prever la conservación general e indiscriminada de las direcciones IP asignadas al origen de la comunicación, siempre que el período de conservación se limite a lo estrictamente necesario. Este es un criterio novedoso, al considerar que las direcciones IP no revelan, como tales, ninguna información sobre terceros que hayan estado en contacto con la persona que realizó la comunicación y son menos sensibles que otros datos de tráfico. Sin embargo, dado que pueden utilizarse para rastrear toda la actividad en línea de un usuario de internet y los da-

tos permiten elaborar un perfil detallado del usuario (apartado 152), solo pueden conservarse para casos de delincuencia grave.

Por primera vez el Tribunal reconoce que, cuando se comete un delito en línea, la dirección IP puede ser el único medio que permita la investigación de la persona a la que se asignó. Además, esos datos no son necesarios para los proveedores a los efectos de facturación de los servicios que ofrecen (apartado 154), por lo que es la única forma de poder disponer de ellos durante un tiempo, aunque sea limitado a lo estrictamente necesario a la luz del objeto perseguido (apartado 156).

Por lo tanto, la obligación de conservación preventiva de estas para luchar contra la delincuencia grave, prevenir amenazas graves para la seguridad pública y salvaguardar la seguridad nacional puede estar justificada, siempre que el período de conservación no exceda de lo estrictamente necesario a la luz del objetivo perseguido (Apartado 156).

El Derecho de la UE no se opone a las medidas legislativas que prevén, a los mismos fines, la conservación general e indiscriminada de los datos relativos a la identidad civil de los usuarios y abonados (apartado 157). En particular, los Estados miembros no están obligados en este último caso a limitar el período de conservación (apartado 159).

Otra forma de conservación diferente, pero relevante, es la conservación rápida *(quick freeze, en inglés)*. El Tribunal se pronuncia (apartados 160 y siguientes) en el sentido de que el Derecho de la Unión no se opone a una medida legislativa que permita recurrir a la conservación rápida de los datos de que disponen los proveedores de servicios, cuando se produzcan situaciones en las que sea necesario conservar esos datos más allá de los plazos legales de conservación, en caso de delitos graves o de riesgos a la seguridad nacional, cuando ya se hayan cometido o cuando pueda sospecharse su existencia (apartado 164).

En estos casos se permite que los Estados miembros prevean la posibilidad de ordenar, mediante una decisión de la autoridad competente sujeta a control judicial efectivo, la retención rápida de los datos de tráfico y de localización de que dispongan durante un periodo de tiempo determinado. Por tanto, la medida surtirá efecto desde que se obtenga esa autorización, sin poder recurrir a datos anteriores [aunque sean también relevantes e imprescindibles para el caso concreto autorizado]. La solicitud no tiene por qué referirse únicamente a personas sospechosas, también pueden ser relativos a víctimas o zonas geográficas que incluyan el lugar de comisión del delito, etcétera. (apartado 165).

En esta sentencia el TJUE entra a determinar la casuística concreta y a sentar las bases del futuro [si fuera el caso] régimen de conservación de datos, al enumerar de forma exclusiva y casi excluyente los supuestos que habilitan tal medida, incluso aportando supuestos de conservación generalizada e indiferenciada, que en un primer momento declaró contrarios a Derecho respecto de la Directiva 2006/24/CE. Podemos considerar que establece una excepción a su doctrina anterior a través ejemplos [cuestión esta que ha producido sorpresa en parte de los expertos]. Otros, como revela Polo Roca (2021; 12)[69], temen que, con este criterio matizado del Tribunal de Luxemburgo, se esté avalando la vuelta a un régimen de conservación de datos de forma preventiva[70].

2. Sentencia de 2 de marzo de 2021, Caso C-746/18 H.K v. Prokuratuur

La sentencia del 2 de marzo del pasado año, en el *asunto C-746/18 H.K v. Prokuratuur*[71] mantiene también el criterio de que es esencial que el acceso de las autoridades nacionales sea objeto de un control previo por parte de un órgano jurisdiccional/administrativo independiente y que la decisión debe adoptarse tras una solicitud motivada (apartado 51). No obstante, en la investigación penal, el control exige que el órgano jurisdiccional o la entidad estén en condiciones de garantizar un justo equilibrio entre los intereses vinculados a las necesidades de la investigación en materia de lucha contra la delincuencia grave y los derechos fundamentales relacionados con el respeto de la vida privada y la protección de los datos personales, actuando con objetividad e imparcialidad (apartado 52) y llega a la conclusión de que no puede ser el ministerio público —ministerio fiscal— [quien dirige la investigación y ejerce también el poder de decisión con total independencia], sino que debe ser sometido, en su caso, a la consideración de un tribunal competente en el proceso penal. El hecho de que el fiscal esté obligado (en virtud de las normas que regulan sus competencias y su estatuto) a verificar los elementos incriminatorios

---

[69] POLO ROCA, A., «*La regulación sobre la conservación de datos en el sector de las comunicaciones electrónicas o telecomunicaciones: estado de la cuestión*», Revista de los Estudios de Derecho y Ciencia Política, núm. 33, octubre, 2021, págs. 1-16, pág. 12.

[70] Vid. RODRÍGUEZ LAINZ, J.L., «*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. 9740, 2020.

[71] Sentencia TJUE (Gran Sala), de 2 de marzo de 2021, asunto C-746/18, H.K. v. Prokuratuur.

y exculpatorios, a garantizar la legalidad de la investigación y actuar únicamente conforme a la ley, no basta para conferirle la condición de tercero en relación con los intereses afectados.

3. Más dudas, mismas respuestas

a) Sentencia de 5 de abril de 2022, Caso G.D y Commissioner of An Garda Síochána

Este mismo año (2022), el 5 de abril pasado, se publica una nueva sentencia del Tribunal europeo (Gran Sala)[72], en este caso respecto de una cuestión prejudicial planteada por el Tribunal Supremo de Irlanda (C-140/20). De nuevo Irlanda solicita el parecer el Alto tribunal, pero esta vez respecto de un proceso civil dirigido a solicitar la invalidez de determinadas disposiciones de su normativa nacional de transposición (Ley de 2011) de la Directiva de conservación de datos. En esta ocasión, anulada la directiva de 2006, se pretendía confrontar la ley nacional con la habilitación prevista en el artículo 15, apartado 1, de la Directiva 2002/58/CE.

El tribunal irlandés albergaba todavía dudas sobre las exigencias del Derecho de la Unión respecto de la conservación de datos con fines de lucha contra la delincuencia y argumenta que «*solo una conservación generalizada e indiferenciada de los datos […] permite luchar eficazmente contra la delincuencia grave y que, en cambio, una conservación selectiva y una conservación rápida no resultarían tan eficaces*». Además, respecto de la conservación selectiva, cuestiona la posibilidad de centrarse en grupos o zonas geográficas determinados a efectos de la lucha contra la delincuencia grave, «*en la medida en que ciertos delitos graves rara vez implican circunstancias que las autoridades nacionales competentes conozcan y que permitan a estas sospechar con anticipación la comisión de un delito, además de que una conservación selectiva pueda dar lugar a discriminaciones. En cuanto a la conservación rápida, considera que solo es útil en situaciones en las que existe un sospechoso que puede ser identificado en una fase temprana de la investigación*» (apartado 26).

En esta sentencia el Tribunal reitera su pronunciamiento de 2020 (*La Quadrature du Net y otros)*. Nos llama la atención que la propia Comisión Europea «*sostuvo que la delincuencia especialmente gra-*

[72] Sentencia TJUE (Gran Sala), de 5 de abril de 2022, en el asunto C-140/20, en https://curia.europa.eu/juris/document/document_print.jsf?docid=257242&text=&dir= .

ve podría asimilarse a una amenaza para la seguridad nacional». Es ciertamente un debate interesante y difícil, no abordado en estudio. Empero, el TJUE diferencia claramente entre el objetivo de la seguridad nacional y de la delincuencia grave, con los mismos argumentos de sentencias anteriores, y descarta que puedan considerarse asimilables[73].

Refuta también el Tribunal el argumento expresado anteriormente, respecto de que solo una conservación generalizada e indiferenciada de estos datos permitiría luchar de forma eficaz contra la delincuencia grave, arguyendo que «*la eficacia de las acciones penales depende generalmente no de un solo medio de investigación, sino de todos los medios de investigación que se hallen a disposición de las autoridades nacionales competentes a los referidos efectos*» (apartado 69).

Respecto de la dificultad para establecer un criterio geográfico a la hora de solicitar una conservación selectiva de metadatos, el Tribunal también aporta un ejemplo concreto de posible criterio que justifique tal medida: «*la tasa media de delincuencia en una zona geográfica*», aunque no se cuente con indicios concretos sobre la preparación o la comisión de delitos graves en esas zonas concretas (apartado 80). Y finaliza traspasando la responsabilidad en la identificación de otros criterios a los Estados miembros, dejando entrever, que estos adolecen de falta de imaginación en la búsqueda de soluciones y, quizás también, una mera resistencia al cambio.

Respecto de la conservación rápida *(quick freeze)*, reitera los argumentos de la sentencia anterior sobre las posibilidades de uso de esta técnica de conservación [antes mencionadas].

Otra cuestión importante que se planteó ante el TJUE (en este caso por el gobierno danés) es la relativa a la posibilidad de que las autoridades nacionales competentes puedan acceder, a efectos de la lucha contra la delincuencia grave, a los metadatos conservados para hacer frente a una amenaza grave a la seguridad nacional que resulte real y actual o previsible y que, en consecuencia, hayan dado lugar a una conservación general e indiferenciada. La instancia europea mantiene su posicionamiento y considera que lo que se está proponiendo es autorizar el acceso de unos metadatos que han sido conservados con un objetivo concreto (una amenaza grave para la seguridad nacional de un Estado miembro) para otro fin distinto (la lucha contra la de-

[73] En el mismo sentido se pronunció también el Abogado General al afirmar que «*tal asimilación podría implicar la introducción de una categoría intermedia entre la seguridad nacional y la seguridad pública para aplicar a la segunda las exigencias inherentes a la primera*».

lincuencia grave) y, por tanto, dependiendo de unas circunstancias ajenas a aquel objetivo. Por lo tanto, no lo «*autoriza*».

Finalmente, cierra la sentencia recordando que la admisibilidad de las pruebas obtenidas mediante el régimen de conservación que rige en un determinado Estado miembro corresponde a estos, de acuerdo con el principio de autonomía procesal.

b) El pronunciamiento más reciente: Caso SpaceNet AG y Telekom Deutschland GmbH, de 20 de septiembre de 2022

La última sentencia[74] resuelve una cuestión prejudicial del Tribunal Supremo de lo Contencioso-Administrativo de Alemania en sendos procedimientos en que empresas de telecomunicaciones germanas (SpaceNet y Telekom Deutschland) recurrieron ante sus tribunales nacionales la obligación de conservación general e indiferenciada que les impone la Ley de Telecomunicaciones alemana[75], durante plazos cortos y limitados[76].

La ley alemana se aprobó en 2004, por tanto, también en transposición de la directiva de 2006. No obstante, el Tribunal Constitucional alemán había declarado nula la norma anterior, por lo que la ley se modificó en diciembre de 2015, para adaptarse al dictamen del Alto Tribunal alemán. Ese es el motivo por el que actualmente incluye algunas características que la diferencian de las de otros Estados miembros[77]. Y esas diferencias, consideramos que son las que han hecho

[74] Sentencia TJUE (Gran Sala), de 20 de septiembre de 2022, en los asuntos acumulados C-793/19 y C-794/19, SpaceNet AG y Telekom Deutschland GmbH.

[75] Ley de Telecomunicaciones, de 22 de junio de 2004.

[76] Cuatro semanas para los datos de localización y diez semanas para los datos de tráfico.

[77] 1.- No se exige la conservación de todos los datos de tráfico relativos a las telecomunicaciones de todos los abonados y usuarios registrados en lo que respecta a todos los medios de comunicación electrónica. Excluye los datos relativos a los sitios de Internet consultados, los datos de los servicios de correo electrónico y los datos en los que se basan las comunicaciones de carácter social o religioso hacia o a partir de determinadas líneas, que no podrán conservarse; 2.- Establece un período de conservación muy inferior al de la mayoría de los Estados miembros y al que posibilitaba la directiva de 2006: cuatro semanas para los datos de localización y diez semanas par los datos de tráfico; 3.- Establece limitaciones estrictas en lo que respecta a la protección de los datos conservados y al acceso a ellos, de tal forma que, según el Tribunal alemán, garantiza una protección eficaz de los datos conservados frente a los riesgos de abuso y de acceso ilícito a los mismos y, por otro, garantiza que su utilización solo podrá serlo para la lucha contra los delitos graves o para la prevención de un riesgo concreto para la integridad física, la vida o la libertad de una persona o para la existencia del Estado federal o de un *Land*.

plantear dudas al Constitucional alemán, por cuanto parece indicar que, a priori, podían ser suficientes para no conculcar los preceptos de la Directiva 2002/58/CE ni provocar una injerencia «*inadmisible*» en los derechos fundamentales de los ciudadanos alemanes.

En este procedimiento, se acordó su suspensión, por estar en una fase más avanzada la resolución del asunto que se sustanció con la *Sentencia La Quadrature du Net y otros* (C-511/18, C-512/18 y C-520/18). De hecho, la mayoría de los argumentos de *La Quadrature du Net* se repiten literalmente en esta sentencia, lo que nos lleva a inferir cuál será el sentido del dictamen de los magistrados del TJUE.

Sobre el alcance de los datos conservados, si bien se excluyen determinadas categorías, considera que los conservados siguen pudiendo permitir extraer conclusiones muy precisas sobre la vida privada de las personas afectadas (apartado 78).

Respecto del período de conservación, reconoce el Tribunal que es «*sensiblemente*» más corto que los previstos en otras normativas nacionales, así como que es este un factor pertinente a tener en cuenta. Sin embargo, a renglón seguido (apartados 87 y 88) [a nuestro entender] le resta toda la importancia, pues declara que «*la gravedad de la injerencia se deriva del riesgo […] de que estos permitan extraer conclusiones muy precisas sobre la vida privada de la persona […]*» y concluye que «*la conservación de los datos de tráfico o de localización […] es, en todo caso, grave, con independencia de la duración del período de conservación, […]*»[78].

VII. EL CAMBIO DE PARADIGMA INTRODUCIDO POR EL TRIBUNAL EUROPEO

A raíz de la decisión del Tribunal de Justicia declarando la invalidez *ab initio* de la Directiva 2006/24/CE *sonaron las alarmas* en los Estados miembros, aduciendo que se dificultaría la realización eficaz de las investigaciones penales y, en 2017, se puso en marcha un proceso de reflexión en el seno del Consejo de la UE sobre cómo avanzar[79] y con el objetivo de explorar posibles soluciones para garantizar la

[78] Remite el TJUE a ver la Sentencia de 2 de marzo de 2021, Prokuratuur, C-746/18, EU:C:2021:152, apartado 39.

[79] Los ministros encomendaron al Grupo de «*Intercambio de Información y Protección de datos -DAPIX: Amigos de la Presidencia*» que estudiara cualesquiera opciones legislativas y no legislativas, también en el contexto de la propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas, y que evaluara la viabilidad de estas con vistas a abordar las cuestiones derivadas de la jurisprudencia del TJUE.

disponibilidad de datos con fines de la prevención y la lucha contra la delincuencia grave. La institución europea valoró entonces los efectos de la sentencia y consideró que no había más remedio que realizar una evaluación estricta de la proporcionalidad y de la necesidad de las medidas que se adopten, pero que nunca podrían estas constituir graves restricciones de los derechos fundamentales, aunque sean legítimos los objetivos perseguidos; así como que debían establecerse salvaguardias adecuadas respecto de las medidas de conservación que se aprueben[80].

Es cierto que, con el paso del tiempo, los cuerpos policiales han ido adaptando sus métodos y técnicas de investigación para el esclarecimiento de los delitos y, en la sociedad de la información en que vivimos, con una *excesiva* interdependencia y conectividad entre los ciudadanos, las autoridades han tenido que reaccionar [muchas veces tarde o demasiado lento] para poder aprovechar la ingente cantidad de información que se genera y se comparte, también a esos fines de esclarecimiento y enjuiciamiento de los delitos, hasta el punto que para algunos autores se ha llegado a una situación de «*tecnovigilancia*»[81], y se ha avanzado a un ritmo desigual entre el empleo de técnicas de investigación de este tipo y la elaboración de una legislación adecuada y actual que respalde esa actuación. Quizás esta dependencia justifica en parte la gravedad de la situación creada por el Tribunal europeo, hasta el punto de que ha supuesto una labor difícil y hasta la fecha no muy productiva, para poder aprobar una nueva norma europea sobre la conservación y acceso a los datos de las comunicaciones electrónicas que sea conforme con la jurisprudencia del Tribunal europeo y satisfaga las necesidades de los ciudadanos, respecto de las misiones que estos han adjudicado a las agencias encargadas de la aplicación de la ley.

En esta accidentada carrera de obstáculos propiciada por el Alto Tribunal europeo, hasta la fecha todo han sido dificultades: por un lado, la correspondiente al acceso limitado a los datos y, por otro [y quizás más grave, por cuanto sin este paso no se puede producir el anterior] la relativa al establecimiento de la forma de conservación (la conservación selectiva). Mientras tanto, los cuerpos policiales com-

[80] Consejo de la Unión Europea, en «*Judgment of the Court of 8 April 2014 in joined Cases C-293/12 and C-594/12, 9009/14*», Brussels, 5 May 2014, Exchange of views between Commissioner Dimitris Avramopoulos and MEPs at the LIBE Committee in the European Parliament, 3 December 2014, en http://europa.eu/rapid/press-release_SPEECH-14-2351_en.htm .

[81] ORTIZ-PRADILLO, J.C., «*Europa: auge y caída de las investigaciones penales...*» op. cit., pág. 10

prueban como se desmorona uno de los elementos de investigación principales ante muchos delitos. Ortiz-Pradillo[82] (2020; 11) considera que es difícil encontrar una solución al problema si esta ha de venir únicamente a través de la vía interpretativa y no mediante una nueva propuesta legislativa en los Estados miembros.

Lo cierto es que, en base a los casos que exponen los expertos policiales, se observa que una clasificación de los datos por categorías según su importancia no es operativa, ya que la experiencia ha demostrado que las investigaciones comienzan con los datos disponibles para un delito concreto. Los datos disponibles en ese momento serán los considerados como más relevantes, y pueden diferir de un caso a otro. Puede ser una dirección IP, un número de teléfono, un apodo de un usuario en línea, una cuenta en una red social, un monedero de Bitcoin, etcétera.

Teniendo esto en cuenta, consideran que una opción más razonable podría ser aplicar diferentes umbrales a las distintas categorías de datos en función del nivel de interferencia en los derechos de los sospechosos, de las víctimas y, posiblemente también de otras personas no implicadas en los hechos investigados, pero sí relacionadas de alguna forma. Este enfoque, reflejaría los distintos niveles de autorización requeridos, lo que, extrapolado a las investigaciones tradicionales, diferenciaría, por ejemplo, la citación policial frente a la prerrogativa del juez o del fiscal.

Sin duda alguna, defendemos que el punto de partida para un nuevo régimen de conservación de datos deberá atender a los requerimientos del TJUE y, en consecuencia, deberá definir los delitos y las circunstancias específicas para los que se podrán conservar los datos; los tipos de datos que puedan ser conservados; las medidas técnicas, de seguridad y organizativas para el acceso a los datos retenidos y las autoridades que puedan hacerlo; el sistema de autorización y de control que corresponderá a jueces y otras autoridades administrativas con competencia en la materia; procedimientos concretos para realizar la trazabilidad de los accesos; la duración de la conservación en función de los datos concretos y de la gravedad de los delitos para cuya investigación, persecución y enjuiciamiento sobre tratados. Aunque no es objeto de este estudio, también será importante considerar los procedimientos y mecanismos para la transferencia internacional de esos datos.

[82] *Íbid*, op. cit., pág. 11.

Ante la difícil situación creada a raíz de la invalidación de la directiva, la Comisión, como complemento y apoyo a las discusiones que el Consejo había puesto en marcha presentó un concurso para que una consultora realizara un estudio detallado del impacto de la nueva situación en la actuación y labor diaria de los servicios policiales y en el proceso penal. Aunque contó con algunas importantes limitaciones[83], permitió poner de manifiesto algunas cuestiones relevantes, tanto a favor como en contra de nuestros pensamientos iniciales y también de las creencias de los expertos que llevaban ya tiempo discutiendo y valorando opciones para encontrar una solución adecuada. El informe presentó [aunque no disponemos de la información completa ni del parecer de todos los Estados miembros de la Unión] una imagen nítida y, al mismo tiempo, preocupante, sobre las consecuencias de no poder armonizar las reglas sobre conservación de metadatos, así como el acceso a los mismos con fines de investigación penal y enjuiciamiento de delitos; además de que, aunque se homogenicen las normas, no existe información sobre la que realizar una solicitud con autorización judicial, porque los proveedores de servicios no podrán conservar una información muy valiosa, incluso fundamental en algunos delitos concretos a través de los servicios de Internet.

VIII. CONCLUSIONES

Primera. Ocho años después de la primera sentencia, tras la invalidación de la Directiva 2006/24/CE y la confirmación por el TJUE de su doctrina inicial —al margen de la leve modulación de su posición, con introducción de criterios y casuística concretos— es perentorio asumir que la situación no volverá a ser como en 2006, en la medida en la que ya no se aprobará una conservación generalizada e indiferenciada de todos los datos de todas las comunicaciones electrónicas de todos los ciudadanos europeos[84], y buscar alternativas para obtener el mayor beneficio de la nueva realidad. Como indica el

[83] Participaron solo 10 Estados miembros (Austria, Estonia, Francia, Alemania, Irlanda, Italia, Polonia, Portugal, Eslovenia y España) en el estudio, lo que representa solo un 38% de los países que conforman la Unión Europea. Aun así, los países más grandes y próximos también culturalmente a España sí tomaron parte en el estudio. Más importante que lo anterior es la fragmentación de la información aportada, según la consultora por reticencias a compartir información considerada sensible por los participantes. Esto último, una vez más [un ejemplo más] demuestra que no hay una verdadera conciencia europea, por mucho que se utilice la retórica contraria en las reuniones y debates en el seno de las *instituciones* europeas.

[84] Salvo una situación muy específica de un peligro real, previsible e inminente a la seguridad nacional, y bajo unas salvaguardas estrictas.

propio Tribunal, corresponde a los Estados miembros determinar las opciones y posibilidades que permitan luchar de forma eficaz contra la delincuencia grave y otras amenazas de acuerdo con la excepción a la normativa europea vigente sobre privacidad. No obstante, en la medida en que el Tribunal desciende en las sentencias casi al detalle de cómo se reflejarían cada uno de los supuestos en la norma que pudiera aprobarse, hemos de señalar que en los pocos matices que se ofrecen desde la posición inicial hasta la última sentencia, se observan también ciertas incoherencias argumentativas, como el hecho de que uno de los supuestos que le llevaron a considerar la gravedad de la injerencia en los derechos era el periodo de conservación de los datos; sin embargo, cuando la ley alemana se modifica y, buscando subsanar esa deficiencia, introduce periodos de conservación extremadamente cortos (a nuestro entender), el Tribunal se pronuncia indicando que el periodo de conservación no es relevante a los efectos de la injerencia, ya que esta se produce desde el mismo momento en que se conservan los datos.

Segunda. Alargar la situación actual supone mermar las posibilidades de actuación de los servicios policiales y otras autoridades competentes en la defensa de los derechos de los ciudadanos y extender sus efectos adversos a procesos judiciales en curso.

Tercera. Las medidas hacia un nuevo sistema de conservación de metadatos de comunicaciones electrónicas deben inexorablemente partir del consenso entre los colegisladores en las instituciones europeas (Consejo de la UE y Parlamento Europeo) tras una propuesta legislativa de la Comisión que palíe los errores de la de 2006 y con la participación de todos los actores implicados (también el sector profesional afectado y la sociedad civil). Mantener soluciones nacionales, en un entorno global de interdependencia y de supresión de fronteras digitales es del todo inoperativo e ineficiente. Ese fue uno de los motivos que dio lugar a la directiva anulada, y no se puede retornar ahora a soluciones nacionales.

Cuarta. Las leyes nacionales de transposición de la Directiva 2006/24/CE, si bien no pierden su vigencia de forma automática, no deben seguir aplicándose a la luz de las reiteradas sentencias del TJUE. Existe un riesgo cierto de que dilaten la toma de decisiones si se siguen planteando cuestiones prejudiciales y se espera a su resolución ante la esperanza, poco probable, de cambio de criterio del Tribunal y, al mismo tiempo, se pueden *tirar por tierra* muchos procesos judiciales que juzgan delitos muy graves y conductas socialmente muy alarmantes; o incluso la revisión de condenas anteriores o

la indemnización de las víctimas. Además, consideramos que se está trasladando a los proveedores de servicios una responsabilidad de conservación que les genera inseguridad jurídica y eventuales sanciones administrativas y/o penales, tanto si prosiguen con el sistema de almacenamiento de datos como si no lo hacen.

Quinta. Sin cuestionar la obligación de realizar un análisis de necesidad y proporcionalidad a la hora de evaluar la colisión entre derechos fundamentales, consideramos que corresponde a los poderes públicos *esforzarse* más a la hora de adoptar medidas que supongan una injerencia en los derechos civiles de los ciudadanos, pues siempre contarán con más herramientas (como pueden ser las distintas técnicas de investigación y la recolección y aportación de pruebas a un proceso judicial), pero los investigadores y autoridades judiciales deben disponer de las mismas herramientas, como mínimo, de las que se sirven los delincuentes para esconder su identidad y cometer sus acciones, tanto actuales (políticas tendentes a garantizar la privacidad y la protección de los datos de carácter personal) como en un futuro próximo (cifrado de datos, 5G, Internet de las Cosas, etcétera). Creemos que [por suerte] existen controles adecuados y precisos sobre la actuación de los servicios policiales, que no justifican la sospecha de «*tecnovigilancia*» que se quiere proyectar sobre ellos.

Sexta. El impulso principal para llegar a una solución sobre qué camino seguir no depende tanto de los afectados directamente por la aplicación de la norma europea que se apruebe (ciudadanos, sector profesional de las telecomunicaciones o policías y jueces), sino de los decisores políticos y aquellos otros con capacidad legislativa en los Estados miembros, que deben acudir a *Bruselas* con una visión de conjunto y con una apuesta europea y no bajo una visión puramente nacional —todos cedemos para ganar todos— y que deben hacer una propuesta lo antes posible sobre la que modular las posiciones y consensuar las medidas a adoptar. Es imprescindible continuar explorando las posibilidades que ofrece el próximo reglamento sobre privacidad de las comunicaciones —que está en fase de discusión entre los colegisladores— para que recoja la adaptación del vigente artículo 15, apartado 1 de la Directiva 2002/58/CE, e incluya una cláusula general que habilite la adopción de la futura norma de conservación de datos en el ámbito que hemos abordado, respetuosa con los derechos fundamentales recogidos en la Carta y con la jurisprudencia del TJUE, pero igualmente eficaz en la lucha contra la delincuencia grave en la Unión Europea.

BIBLIOGRAFÍA

Alonso García, R., «*Lisboa y el Tribunal de Justicia de la Unión Europea*», Papeles de Derecho Europeo e Integración Regional, Instituto de Derecho Europeo e Integración Regional (IDEIR), Universidad Complutense, núm. 1, págs. 1-30, recuperado en: https://www.UC3M.es/data/cont/docs/595-2013-11-07-lisboa%20y%20el%20derecho.pdf, consultado el 18 de agosto de 2022.

Fernández Ogallar, N., *El derecho penal armonizado en la Unión Europea*, Madrid, Dykinson, 2104.

Fernández Rodríguez, J.J., «*Los datos de tráfico de comunicaciones electrónicas: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente*», Revista Española de Derecho Constitucional, Centro de Estudios Políticos y Constitucionales, págs. 93-122.

López Aguilar, J.F., «*La protección de datos personales en la más reciente jurisprudencia del TJUE: los derechos de la CDFUE como parámetro de validez del derecho europeo, y su impacto en la relación transatlántica UE-EE.UU.*», UNED, Teoría y Realidad Constitucional, núm. 39, 2017, págs. 557-581.

Marsal Muntalá, J., «*Seguridad versus Libertad*», págs. 219-226, recuperado en http://arbor.revistas.csic.es, consultado el 15 de julio de 2022.

Nieves Saldaña, M., «*The right to privacy: la génesis de la protección de la privacidad en el sistema constitucional norteamericano, el centenario legado de Warren y Brandeis*», UNED, Revista de Derecho Político, núm. 85, 2012, págs. 195-240.

Ortiz Pradillo, J.C. «*Europa: auge y caída de las investigaciones penales basadas en la conservación de datos de comunicaciones electrónicas*», Revista General de Derecho Procesal, núm. 52, 2020, págs. 1-28.

Pérez Estrada, M.J., «*La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información*», Universidad del País Vasco, 2019, págs. 1297-1330, recuperado en http://orchid.org/0000-0001-7402-4863, consultado el 18 de julio de 2022.

Pérez Royo, J., «*La democracia frente al terrorismo global*», Terrorismo, democracia y seguridad, en perspectiva constitucional, Barcelona, 2010, págs. 7-12.

Polo Roca, A., «*La regulación sobre la conservación de datos en el sector de las comunicaciones electrónicas o telecomunicaciones: estado de la cuestión*», Revista de los Estudios de Derecho y Ciencia Política, núm. 33, octubre, 2021, págs. 1-16.

Puerto, M.I y Sferrazza Taibi, P., «*La sentencia Schrems del Tribunal de Justicia de la Unión Europea: un paso firme en la defensa del derecho a la privacidad en el contexto de la vigilancia masiva transnacional*», en Revista Derecho del Estado, núm. 40, enero-junio de 2018, págs. 209-236.

Rodríguez Lainz, J.L., *El renacer de la Ley Española sobre conservación de datos relativos a las comunicaciones*, Diario La Ley, núm. 9740, 2020.

Serra Cristóbal, R., «*Los derechos fundamentales en la encrucijada de la lucha contra el terrorismo. Lo que el constitucionalismo y el derecho de la Unión Europea pueden ofrecer en común*», UNED, Teoría y Realidad Constitucional, núm. 38, 2016, págs. 487-503.

Rizzo, G., *Derecho a la privacidad y seguridad en el espacio público europeo*, Tesis doctoral, Universidad Carlos III de Madrid, 2019, recuperado en Derecho a la privacidad y seguridad en el espacio público europeo (uc3m.es), consultado el 2 de septiembre de 2022.

JURISPRUDENCIA Y REFERENCIAS LEGISLATIVAS

Carta de los Derechos Fundamentales de la Unión Europea (2010/C 83/02), de 30 de marzo de 2010.

Convenio para la protección de las personas con respeto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981.

Tratado de Funcionamiento de la Unión Europea, de 30 de marzo de 2010.

Tratado de Lisboa (2007/C 306/01), de 17 de diciembre de 2007.

Sentencia del TEDH, Rotaru, 4 de mayo de 2000, nº 2841/95, 47

Sentencias TJUE de 20 de mayo de 2003, Österreichischer Rundfunk, C-465/00, C-138/01 y C-139/01, Rec. 2003 p. I-4989.

Sentencia del TJUE en el Caso Yasin Adbullah Kadi y Barakaat International Foundation vs. Consejo de la Unión Europea y Comisión de las Comunidades Europeas, de 3 de septiembre de 2008.

Sentencia TJUE, de 10 de febrero de 2009, Irlanda/Parlamento Europeo y Consejo de la UE, C-301/06, Rec. P. I-00593.

Sentencia TJUE del 9 de noviembre de 2010, Volker, C-92/09 y C-93/09.

Sentencia en el Caso Stichting Al-Aqsa vs. Consejo de la Unión Europea y Reino de los Países Bajos contra Stichting Al-Aqsa, de fecha 15 de noviembre de 2012.

Sentencia del Tribunal de Justicia (Gran Sala) de 8 de abril de 2014, en los asuntos C-293/12 y C-594/12.

Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) «Tele 2 and Watson», de 21 de diciembre de 2016, Casos C-203/15 y C-698/15.

Sentencia TJUE Caso C-207/16 Ministerio Fiscal, 2 de octubre de 2018.

Sentencia TJUE (Gran Sala), de 2 de marzo de 2021, asunto C-746/18, H.K. v. Prokuratuur.

Sentencia TJUE (Gran Sala), de 5 de abril de 2022, en el asunto C-140/20.

Sentencia TJUE (Gran Sala), de 20 de septiembre de 2022, en los asuntos acumulados C-793/19 y C-794/19, SpaceNet AG y Telekom Deutschland GmbH.

Conclusiones del Abogado General de la Unión Europea, Sr. Paolo Mengozzi, 8 de septiembre de 2016, Dictamen 1/15.