LOS DATOS DE TRÁFICO DE COMUNICACIONES: EN BÚSQUEDA DE UN ADECUADO RÉGIMEN JURÍDICO QUE ELIMINE EL RIESGO DE CONTROL PERMANENTE

Communication Traffic Data. In Search of a Suitable Legal Regime for Removing the Risk of Permanent Control

JOSÉ JULIO FERNÁNDEZ RODRÍGUEZ
Universidad de Santiago de Compostela
josejul.fernandez@usc.es

Cómo citar/Citation
Fernández Rodríguez, J. J. (2016).
Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente.
Revista Española de Derecho Constitucional, 108, 93-122.
doi: http://dx.doi.org/10.18042/cepc/redc.108.03

Resumen

En el presente artículo se analiza, jurídicamente, el problema de la retención de datos de tráfico de comunicaciones partiendo de la injerencia que supone sobre derechos como la intimidad, la protección de datos, el secreto de las comunicaciones y, eventualmente, la libertad de circulación. Frente a ello, la normativa y los decisores públicos esgrimen razones de seguridad para enfrentarse al crimen y al terrorismo. La anulación de la Directiva 2006/24/CE insiste en este debate. La Ley española 25/2007 regula esta retención, para nosotros con ciertas carencias que recomiendan su reforma. Se trata, en definitiva, de lograr un adecuado equilibrio entre la seguridad y la libertad, verdadera clave del presente para lograr una adecuada convivencia.

Palabras clave

Secreto de las comunicaciones; intimidad; datos de tráfico y localización; libertad; seguridad.

Abstract

This article analyzes, from a legal point of view, interference that communication traffic data retention entails with rights to respect for privacy, data protection, communications privacy and, conditionally, freedom of movement. In this matter, legislation and public policy argue security reasons in order to face up to crime and terrorism. The declaration of invalidity of Directive 2006/24/CE keep the debate alive. The Spanish Law 25/2007 on retention of data has certain shortcomings which require changes. In short, it's a question of searching of the suitable balance between security and freedom, that is nowadays the key issue for democratic coexistence.

Keywords

Communications privacy; traffic and location data; privacy; freedom; security.

SUMARIO

Y ha estado, con todos los demás, de parte del poder,
(del poder que uno tiene, o del que tan solo participa: no tiene importancia).

Pasolini (1996: 36)

I. INTRODUCCIÓN

1. EL DESAFÍO DIGITAL

Vivimos en un mundo nuevo, el mundo digital, que ha tenido múltiples repercusiones en diversos ámbitos. Tales incidencias también han afectado, por supuesto, al derecho, que se ve obligado a reaccionar con prontitud para mantener operativos sus modos de regulación de la sociedad, en especial, las garantías de los derechos fundamentales. En este sentido, son varias las cuestiones problemáticas en semejante interacción entre los derechos fundamentales y las nuevas tecnologías, ya que se ven comprometidos relevantes aspectos de la intimidad, de la libertad de expresión, de la educación o de la participación. Surgen, así, un cúmulo de retos que el jurista debe analizar para adaptar o actualizar las categorías implicadas al nuevo contexto[1].

En esta ocasión pretendemos reflexionar sobre un tema que ha estado abierto durante los últimos años y sobre el que parece que hay una mayor claridad en el momento actual, aunque la legislación sigue sin ayudar. Noso-

[1] Permítasenos remitir a uno de nuestros trabajos: Fernández Rodríguez (2004a). En él ya habíamos intentado avanzar en dicha adaptación.

tros, tiempo atrás, ya criticamos alguna cuestión a este respecto[2]. Habida cuenta de la trascendencia que pueden tener los datos de tráfico de una comunicación, semeja oportuno efectuar en este lugar un análisis específico desde la perspectiva jurídica constitucional. El tema es abigarrado, como una lógica consecuencia del proceloso encuentro ente la tecnología digital y los desafíos de la seguridad.

2. *EXCURSUS* CONCEPTUAL

Para poder articular nuestro discurso es preciso fijar su objeto desde el primer momento, por lo que abrimos un apartado con dicha finalidad, a sabiendas, como señala Requejo Pajés, que «definir supone siempre sustraer», una labor de selección que lleva a desatender ciertas magnitudes[3].

Los datos de tráfico, o metadatos, en una comunicación son los datos que rodean el mensaje que se transmite, pero que no forman parte de dicho mensaje[4]. Son un subproducto de las conexiones, que se concretará en función del tipo de comunicación. Así, en una llamada telefónica, se trata del número de teléfono de llamada, el nombre y la dirección del abonado de origen, el número de destino y el nombre y dirección del abonado de destino, la fecha y hora del comienzo y fin de la comunicación, el servicio telefónico utilizado, y otros datos específicos de la telefonía móvil (la identidad internacional del abonado [lMSI] que llama y del que recibe la llamada; la identidad internacional del equipo móvil [IMEI], también del que llama y del que recibe la llamada; si el servicio es de pago por adelantado: fecha y hora de la primera activación del servicio y la etiqueta de localización o identificador de celda desde la que se haya activado el servicio). En cambio, en el acceso a internet y en el correo electrónico serán metadatos, tanto para el origen como para el destino de la comunicación, la identificación de usuario asignada, el nombre y la dirección del abonado o usuario al que se le ha atribuido una

---

2 En concreto en Fernández Rodríguez (2012: 65 y ss.)

3 Requejo Pajés (1993: 115).

4 El art. 588 ter b) de la Ley de Enjuiciamiento Criminal, introducido por la LO 13/2015, de modificación de aquella para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, preceptúa que «se entenderá por datos electrónicos de tráfico o asociados, todos aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas, de su puesta a disposición del usuario, así como de la prestación de un servicio de la sociedad de la información o comunicación telemática de naturaleza análoga».

dirección de protocolo internet (IP); la fecha y hora de conexión y desconexión del servicio de acceso a internet; el servicio de internet utilizado; o la línea digital de abonado (DSL). Téngase en cuenta que la dirección del protocolo internet puede ser dinámica o estática, en función de la asignación que realiza el proveedor de acceso. Estamos incluyendo parte de los datos de localización en los datos de tráfico, porque son tratados en la conducción de una comunicación.

Como se ve, estos datos accesorios a la comunicación detallan quién, cuándo, dónde y con quién se produce esta sin entrar en su contenido. En general estamos ante unos datos de abonados y usuarios que son necesariamente tratados por los proveedores de comunicaciones para efectuar la propia comunicación, pero que son susceptibles de ser usados de formas muy diferentes, a la vez que pueden agredir los derechos fundamentales.

Téngase en cuenta que los metadatos aluden a una comunicación concreta, siendo diferentes a otros datos o circunstancias personales que tendrán los operadores, pero que son autónomos y se hallan desconectados de una comunicación (esta distinción también se refleja en alguna jurisprudencia, como en la Sentencia del Tribunal Supremo español 247/2010, de 18 de marzo, FJ 3). De todos modos, alguno de estos datos de suscripción o abonado podrían ser también datos de tráfico al ser tratados como tales en el curso de una comunicación.

II. RIESGOS Y AMENAZAS EMERGENTES: LA COMPLEJIDAD DE LA SEGURIDAD ACTUAL

Resulta evidente que la seguridad es una cuestión clave para conseguir una adecuada calidad democrática. Solo en un contexto razonable de seguridad pueden ejercitarse realmente los derechos fundamentales[5]. Los ataques

[5] La relación entre seguridad y derechos fundamentales es ciertamente compleja y presenta múltiples aristas y aspectos. En un esfuerzo de simplificación, podemos señalar dos grandes líneas en dicha relación: por un lado, una relación en negativo y, por otro, en positivo. La primera alude a una dialéctica contrapuesta entre seguridad y libertad, de manera tal que el aumento de una mengua a la otra. En el sentido positivo la relación entre ambas categorías es complementaria: a mayor seguridad, mejor ejercicio de los derechos. Como indica Brandariz García, el art. 17.1 de la Constitución española plasma el entendimiento de la *seguridad* y *libertad* como conceptos sinérgicos, aunque él considera su relación tendencialmente contradictoria (Brandariz García, 2014: 315).

terroristas que periódicamente atentan contra la humanidad lo ponen una y otra vez de manifiesto.

Así las cosas, la seguridad se presenta como una categoría que puede limitar los derechos de forma legítima. Ello es así desde el propio origen del estado constitucional. Atrás quedan visiones idealizadas que concebían los derechos como elementos absolutos que no podían ser limitados. La normativa ofrece abundantes ejemplos que amparan las restricciones por razones de seguridad, tanto en ámbitos estatales como internacionales[6]. Y ello tanto en el sentido de seguridad nacional —es decir, la que se refiere a una escala más amplia, de seguridad del estado, que trata de proteger la existencia del propio estado o del sistema público democrático— como en el de seguridad pública o ciudadana, que se conecta con las investigaciones tendentes a la persecución de los delitos.

En los últimos años, sobre todo tras el fin de la bipolaridad y el ocaso de la guerra fría, nos hemos topado, en un entorno asimétrico, con una serie de riesgos y amenazas emergentes que complica e intensifica la relevancia de las cuestiones de seguridad. Estas últimas ocupan un lugar preponderante en las agendas de los responsables públicos. Nos referimos a cuestiones de primer orden como el terrorismo radical, los Estados fallidos, las armas de destrucción masiva o la inmigración descontrolada. No cabe duda de que el discurso constitucional debe considerar estos riesgos y amenazas para, por un lado, ofrecer respuestas a estos y, por otro, impedir que las visiones fatalistas supongan un coste desproporcionado a la libertad[7].

En este contexto, se produce, por momentos, un intenso diálogo entre la seguridad y la libertad en búsqueda del equilibrio satisfactorio en la sociedad de referencia. No obstante, ha existido la sensación de que la primera categoría, la seguridad, ha sido preponderante en demasía, al menos en algunos momentos. Estamos pensando, por ejemplo, en las reacciones en Estados

---

6 En la escena internacional, sirven de ejemplos los arts. 8, 10 y 11 del Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales, donde se habla de la protección de la seguridad nacional, de la seguridad pública, de la defensa del orden y de la prevención del delito; el art. 29.2 de la Declaración Universal de Derechos Humanos, que alude a las exigencias del orden público en las limitaciones establecidas por ley para el ejercicio de los derechos; los arts. 12.3, 19.3, 21 y 22 del Pacto Internacional de Derechos Civiles y Políticos, que se refieren a seguridad nacional y orden público; y el art. 18.3 de dicho Pacto, que menciona la seguridad y el orden.

7 Desde un punto de vista prospectivo y multidisciplinar, *vid.* Fernández Rodríguez, Jordán Enamorado, Sansó-Rubert Pascual (2008). Acerca del trascendente tema de la vigilancia masiva de comunicaciones, *vid.* Salamanca Aguado (2014).

Unidos tras el 11-S. Nos hallamos realmente ante el verdadero reto del presente: lograr el equilibrio entre seguridad y libertad sin renunciar a una verdadera vigencia de los derechos fundamentes, elementos nucleares de nuestra constitución material y base de sustentación de nuestra forma de convivencia. He aquí una tarea de singular exigencia que debemos abordar los constitucionalistas para ofrecer respuestas cabales a quienes toman las decisiones.

III. LA IMPORTANCIA DE LOS DATOS DE TRÁFICO Y SU CALIFICACIÓN JURÍDICA

Los datos de tráfico no resultan, ni mucho menos, inocuos. La información que contienen puede ser, jurídicamente hablando, muy incisiva. La tecnología digital que se emplea exacerba todos los peligros, tanto a la hora de recabar los datos como en el momento de enviarlos a distancia de una manera masiva, eficaz y barata.

Así las cosas, tanto de forma aislada, pero sobre todo en conjunto, revelan aspectos de la vida privada y de la intimidad. Quién se ha comunicado con quién, con qué frecuencia, en qué momento y de qué modo. Ello muestra hábitos de vida cotidiana y relaciones sociales, conocidas o no, de una persona. De igual forma, contienen datos personales en tanto en cuanto algunos de ellos identifican o hacen identificables a personas. Del mismo modo, inciden en la libertad de expresión y la participación: un individuo que sabe que se recaban esos datos puede autocensurarse a la hora de efectuar una comunicación o de establecer ciertas iniciativas públicas. Por si esto no fuera suficiente también pueden afectar a la libertad de circulación. Téngase en cuenta que los *smartphone* o *tablets* contienen un sistema de GPS que sitúa con precisión la ubicación del aparato[8]. La geolocalización es uno de los aspectos más inquietantes —que merecería nuevos análisis jurídicos que trataremos de efectuar en otro momento—. De este modo se sabe el lugar desde dónde se efectúa la comunicación y, a partir de ahí, los lugares de residencia y los desplazamientos. Frente a esta situación se puede defender la existencia de un derecho a no estar localizado de manera continua[9].

---

8 Algo similar acontece con las balizas rastreadoras que se pueden pegar a un objeto, y que son usadas con normalidad por las fuerzas y cuerpos de seguridad. La Ley de Enjuiciamiento Criminal, tras su reforma de 2015 —*vid.* nota 4—, ofrece por fin una regulación de estas cuestiones (art. 588 quinquies b).

9 Velasco Núñez (2014).

En Estados Unidos hace tiempo que se considera que los métodos tecnológicos no invasivos *(nontrespassory surveillance techniques)* afectan a las expectativas razonables de privacidad de la persona, siendo capaces de ofrecer detalles sobre sus asociaciones familiares, políticas, profesionales, religiosas o sexuales. Resulta elocuente en este sentido, con respecto a la monitorización del GPS, la opinión concurrente de la jueza Sotomayor en el Caso United States *vs.* Jones, 10 U.S. 1259 (2011). No cabe duda de que cada vez son más cotidianas las aplicaciones de monitoreo, que ya resultan baratas y de manejo sencillo.

El actual estado de la técnica permite afirmar con rotundidad que ciertas formas de utilización de los datos de tráfico crean un verdadero riesgo de control permanente de la persona. La interconexión de la distinta información que aportan, que por separado puede resultar intranscendente, da lugar a que se logren establecer precisos perfiles individuales, que son susceptibles de ser usados para múltiples fines.

El encaje jurídico de todo ello, en el sistema constitucional español, es diverso. Está claro que los metadatos afectan al derecho a la intimidad del art. 18.1 de la Carta Magna y a la libertad de expresión de su art. 20. En algún caso afectarán al derecho a la protección de datos derivado del art. 18.4 de la Constitución (cuando identifiquen personas), y en otros supuestos a la libertad de circulación del art. 19 de dicho texto (cuando indiquen ubicaciones). En todo caso, esta parcelación puede resultar un tanto artificial, además de compleja, como dice López-Barajas[10].

Podría parecer dudosa la afectación del art. 18.3, que versa sobre el derecho al secreto de las comunicaciones[11]. Los datos de tráfico no permiten conocer el contenido del mensaje, por lo que el contenido esencial de ese derecho no se ve afectado. De esta forma, en una primera aproximación, semeja que no integran el derecho al secreto de comunicaciones. Sin embargo, alguno de esos datos nos hace pensar lo contrario. Nos referimos a la identidad de los

[10] López-Barajas Perea (2011: 195). Rodríguez Lainz apunta que la incidencia de los diferentes regímenes es tal que pueden llegar a confluir (2003: 447 y ss.).

[11] Como es sabido, la Constitución exige autorización judicial para su limitación por medio de una intervención de comunicaciones. En cambio, nada se dice en este sentido para las inmisiones en el derecho a la intimidad, la protección de datos o la libertad de circulación. Ello no significa que en ciertas inmisiones no sea conveniente contar con dicha autorización. Un principio de precaución garantista así lo aconseja, al igual que el monopolio jurisdiccional en la limitación de los derechos fundamentales. El Tribunal Constitucional solo ha admitido de forma excepcional que la policía judicial realice injerencias leves en la intimidad de las personas sin autorización judicial (SSTC 37/1989, FJ 7; 207/1996, FJ 3; 70/2002, FJ 10).

comunicantes (precisemos: identifican las terminales de los interlocutores, de lo cual se puede derivar racionalmente, en la mayoría de los casos, quienes son dichos interlocutores). Ello nos inclina a defender que la conservación también afecta al secreto de las comunicaciones, lo cual es un salto de relevancia, pues dicho secreto es mucho más que una garantía individual al atesorar una transcendental dimensión objetiva[12]. Para nuestra jurisprudencia constitucional el secreto cubre tanto el contenido de la comunicación como la identidad subjetiva de los interlocutores (SSTC 114/1984, FJ 7; 123/2002, FJ 5; 56/2003, FJ 2; 230/2007, FJ 2), aunque es cierto que se reconoce que la injerencia es de menor intensidad cuando no se accede al contenido (SSTC 123/2002, FJ 6; 56/2003, FJ 3). También el Tribunal Europeo de Derechos Humanos (TEDH) ha visto vulneración de este derecho cuando se conoce con quién o con qué número se comunica (TEDH, Caso Valenzuela Contreras *vs.* España, Sentencia de 30 de julio de 1998, apartado 47; Caso Malone *vs.* Reino Unido, Sentencia de 2 de agosto de 1984, apartado 84). En el mismo sentido, el Tribunal Constitucional alemán considera que una orden judicial que exige dar información sobre los datos de conexión *(Verbindungsdaten)* incide en el derecho a la inviolabilidad de las telecomunicaciones (BVerfGE 107, 299: «*Die gerichtlich angeordnete Auskunft über die Verbindungsdaten der Telekommunikation berührt allerdings den Schutzbereich des Fernmeldegeheimnisses*»). A un mayor abundamiento, en el tema de los datos de tráfico están presentes dos de los argumentos de fondo que sostienen las garantías del secreto de las comunicaciones: estos datos se ubican en canal cerrado y sobre ello el emisor tiene expectativa de privacidad.

Aunque la comunicación ya se haya producido, y el dato de tráfico de la identidad de los interlocutores esté guardado en una base de datos, consideramos que sigue presente la problemática del secreto de las comunicaciones, porque esa identidad se deriva de una comunicación concreta[13]. Es cierto que la doctrina española asentada entiende que finalizada la comunicación la pro-

[12] El Tribunal Constitucional español, hace más de diez años, ya afirmó que «en una sociedad tecnológicamente avanzada como la actual, el secreto de las comunicaciones constituye no solo garantía de la libertad individual, sino instrumento de desarrollo, cultural, científico y tecnológico colectivo» (SSTC 123/2002, FJ 5; 56/2003, FJ 3).

[13] Otra cosa es que se presenten irregularidades a la hora de aportar esos datos a un proceso, en cuanto a su integridad o suficiencia, con lo que aparecerá en escena el derecho a la tutela judicial efectiva, y no el secreto de las comunicaciones (esta idea, referida a la aportación de resultados de intervenciones de comunicaciones, la maneja la Sentencia del Tribunal Supremo 7/2014, de febrero, FJ 2.A.d, siguiendo la STC 126/2000, FJ 9).

tección vendrá por la intimidad u otros derechos (STC 70/2002, FJ 9, c), pero el desbordamiento que supone el entrecruzamiento digital información aconseja que el secreto de las comunicaciones no desparezca de los datos de tráfico, abriendo, así, la dimensión de ese derecho, como por cierto mantiene el TEDH.

Por lo tanto, en función del dato ante el que estemos la calificación jurídica será una u otra. De este modo, creemos que hay datos de tráfico que integran el derecho al secreto de las comunicaciones y otros que simplemente afectan a la intimidad, la protección de datos o la libertad de circulación. Entre los primeros se halla la identidad de los interlocutores de la comunicación. En cambio, la duración de la llamada o la localización de los interlocutores estarán en el ámbito del derecho a la intimidad.

No cabe duda de que esta posición mantenida por nosotros, de diferenciar entre los tipos de datos de tráfico, complica su régimen jurídico. Ello reclama una especial atención, tanto al legislador como al operador jurídico. De todos modos, esta cuestión puede relativizarse, pues en el ámbito europeo los metadatos de un tipo u otro afectan al art. 8.1 del Convenio Europeo de Derechos Humanos, que, como es sabido, tiene un ámbito de protección diferente a nuestros preceptos constitucionales 18.1 y 18.3 separadamente considerados.

IV. ¿NECESIDAD DE CONSERVACIÓN? ACERCA DE SU RÉGIMEN JURÍDICO

Sentados los conceptos de partida y la relevancia del tema que nos ocupa, damos un paso más en nuestra argumentación para reflexionar sobre la problemática de la conservación.

1. ¿CONSERVAR?

Tal vez la cuestión inicial, de la que se derivarían las demás, está en determinar si en realidad es necesaria o no la conservación de los datos de tráfico por razones de seguridad[14].

[14] Téngase en cuenta que la conservación de datos es diferente a su preservación: en esta los operadores notificados por una orden judicial deben guardar datos de determinados individuos, que son sospechosos en la fecha en que se dicta esa orden. La preservación de datos es uno de los instrumentos de investigación que se prevén en el Convenio del Consejo de Europa sobre ciberdelincuencia (art. 16). En cambio, sí

Por motivos técnicos y mercantiles sí es preciso conservar durante un tiempo alguno de estos datos. Eso nadie lo pone en duda, pues de otra forma no sería posible efectuar la comunicación ni la facturación. Las empresas de telecomunicaciones tienen que saber qué tipo de llamadas se efectúan desde los terminales para conducir la comunicación y para cobrar dicho servicio. El propio contrato que un usuario establece con la operadora ampara esa posibilidad[15]. El aspecto problemático, por lo tanto, no es ese, sino la retención global de los datos por razones de seguridad y de manera preventiva.

En una visión cabal del actual contexto, con la presión de los riesgos y amenazas que comentamos antes, que pueden deteriorar en grado sumo nuestra forma democrática de convivencia, la respuesta general a la pregunta de este subepígrafe debe ser positiva. Los datos relativos a las comunicaciones pueden servir de manera especialmente valiosa en las investigaciones que atañen a la delincuencia organizada y el terrorismo. La Declaración sobre la lucha contra el terrorismo, que toma el Consejo Europeo el 25 de marzo de 2004, aconsejó estudiar medidas para establecer normas de conservación de datos de tráfico por parte de los prestadores de servicios. Además, desde diversas instancias se ha subrayado la eficacia de proceder a esta conservación, aunque bien es cierto que tras algún ataque terrorista (como en julio de 2005 después de los atentados en Londres), quizá movidos más por la presión del momento que por un profundo análisis reflexivo.

Está claro que en la lucha contra el terrorismo todos los Estados europeos están implicados, lo que se convierte en un objetivo de interés general de la Unión Europea (Tribunal de Justicia de la Unión Europea [TJUE], Caso Yassin Abdullah Kadi y Al Barakaat International Foundation *vs*. Consejo de la Unión Europea y Comisión de las Comunidades Europeas, Sentencia de 3 de septiembre de 2008, apartado 363; TJUE, Caso Stichting Al-Aqsa *vs.* Consejo de la Unión Europea y Reino de los Países Bajos contra Stichting Al-Aqsa,

---

vamos a usar como sinónimos las palabras conservación y retención (esta última podía entenderse como la preservación señalada, pero nosotros no lo hacemos así).

15 La Ley 9/2014, de Telecomunicaciones, en su art. 48.2.a), permite el tratamiento de los datos de tráfico «necesarios a los efectos de la transmisión de una comunicación»; y los necesarios «a efectos de la facturación de los abonados y los pagos de las interconexiones» hasta que expire «el plazo para la impugnación de la factura del servicio, para la devolución del cargo efectuado por el operador, para el pago de la factura o para que el operador pueda exigir su pago». Cuando tales datos de tráfico dejan de ser necesarios para la transmisión o facturación los usuarios tienen el derecho de que los mismos se hagan anónimos o se cancelen. Esta previsión se entiende «sin perjuicio de las obligaciones establecidas en la Ley 25/2007», de Conservación de Datos Relativos a las Comunicaciones Electrónicas (art. 48.4), a la que luego nos referiremos.

Sentencia de 15 de noviembre de 2012, apartado 130). Algo similar puede afirmarse en la lucha contra la delincuencia grave. En este sentido existe un derecho fundamental a la seguridad, reconocido *de lege data* (por ejemplo, el art. 17.1 de la Constitución española o el art. 6 de la Carta de Derechos Fundamentales de la Unión Europea), imprescindible para el sustento de un régimen democrático. Sin una seguridad suficiente no hay libertad. Existe, por tanto, un objetivo de interés general en la injerencia que implica la conservación, que cubre la finalidad pública perseguida con dicha injerencia. En esta línea, la conservación puede entenderse adecuada para lograr ese objetivo de interés general señalado. Los datos conservados son valiosos para los enjuiciamientos e investigaciones penales al permitir establecer pistas sobre un delito, excluir a sospechosos, confirmar coartadas, contactar con testigos o iniciar investigaciones penales.

De todos modos, la relevancia de la conservación para las investigaciones no debe dar lugar a la pérdida de nuestra perspectiva como juristas. Realmente la conservación por sí misma es una injerencia en los derechos relacionados con la vida privada, al margen del carácter sensible o no de los datos (TJUE, Caso Rechnungshof contra Österreichischer Rundfunk y otros, y Christa Neukomm y Joseph Lauermann *vs.* Österreichischer Rundfunk, Sentencia de 20 de mayo de 2003, apartado 75). Y el acceso de las autoridades públicas, a mayores del acceso de los proveedores de comunicaciones, resulta una inmisión adicional (TEDH, Caso Rotaru *vs.* Rumanía, Sentencia de 4 de mayo de 2000, apartado 46; Caso Weber y Saravia *vs.* Alemania, Sentencia de 29 de junio de 2006, apartado 79). O sea, que la conveniencia de la retención, como un instrumento preventivo, desde la perspectiva de la seguridad nacional y ciudadana, no puede ocultar lo comentado antes con relación a la transcendencia de los metadatos para la vida de las personas. De lo que se trata es de buscar el necesario equilibrio ente los distintos intereses en juego, que es lo que intentamos más abajo, desde la razonabilidad y la proporcionalidad. La tarea es, sin duda, ímproba, pues como afirma 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[16].

En suma, en un entorno como el actual, de amenazas y riesgos múltiples, la balanza se inclina del lado de la lucha contra el terrorismo y la delincuencia organizada, aunque con la necesidad de articular las debidas garantías en ello, para lo cual los márgenes son estrechos, ya que estamos ante verdaderas inje-

[16] En el diálogo mantenido con Fernando Schüler y Mario Mazzilli, que puede verse en la red: https://www.youtube.com/watch?v=in4u3zWwxOM (visionado el 13 de abril de 2015).

rencias en derechos fundamentales. Apoyarse en estos derechos servirá para encontrar la solución correcta pues, como afirma Rubio Llorente, los derechos fundamentales aseguran «el dinamismo social en la búsqueda de una situación más perfecta»[17].

2. LA SITUACIÓN EN LA UNIÓN EUROPEA, CON PECULIAR REFERENCIA A LA POSICIÓN DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

Recordemos sucintamente ahora, y de manera selectiva, la abigarrada normativa de la Unión Europea que se conecta con lo que nos ocupa en el presente trabajo. En ella existen (o existían, mejor dicho) tres niveles de regulación que se refieren a los metadatos, todos en forma de directiva: una previsión general sobre tratamiento de datos, otra más concreta en las comunicaciones electrónicas, y una específica de conservación de datos (que ha sido anulada).

El primero de esos niveles lo constituye la antigua Directiva 95/46/CE, 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, que establece, en su art. 17.1, las medidas de seguridad en el tratamiento de dichos datos. En concreto exige que los Estados miembros impongan esas medidas a los responsables de tratamiento para proteger tales datos frente a su posible destrucción o pérdida, y frente a su alteración, difusión o acceso no autorizado[18].

En esta línea, y conformando el segundo nivel indicado, también se sitúa la Directiva 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. En su art. 5 establece que los Estados miembros garantizarán «la confidencialidad de las comunicaciones, y de los datos de tráfico asociados a ellas» y prohibirán

---

17 Rubio Llorente (1993: 630).

18 El 24 de mayo de 2018 se comenzará a aplicar el nuevo Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, que sustituirá a esta Directiva. De todos modos, la cuestión no cambia en lo estamos diciendo ahora, pues dicho Reglamento mantiene, e incrementa, las obligaciones de protección de los datos, además de incluir novedades como el derecho al olvido (art. 17) o el derecho a la portabilidad (art. 20). El art. 23 permite limitaciones a los derechos establecidos si son una medida necesaria y proporcionada para salvaguardar, entre otras cosas, la seguridad del estado, la defensa y la seguridad pública; y para la prevención, investigación, detección o enjuiciamiento de infracciones penales. Con relación a esto último, las infracciones penales, este Reglamento no se aplicará al tratamiento de datos que hagan las autoridades competentes en ese campo, pues la norma que se aplica es la Directiva específica para ello, la 2016/680, del Parlamento Europeo y del Consejo.

la escucha, la grabación, el almacenamiento y otros tipos de intervención o vigilancia. Fuera de ello queda el almacenamiento técnico necesario para la conducción de una comunicación y, también, la excepción que figura en el art. 15. Asimismo, en el art. 6.1, se prevé que los datos de tráfico de los abonados y usuarios «deberán eliminarse o hacerse anónimos cuando ya no sean necesario a los efectos de la transmisión de una comunicación». Se vuelve a exceptuar el art. 15.1. Este art. 15.1 de la Directiva 2002/58 permite a los Estados miembros adoptar medidas para limitar el alcance de esas previsiones anteriores «cuando tal limitación constituya una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos». Para ello, se permite a los Estados miembros, por ley, establecer la conservación de datos durante un plazo limitado, justificado por los motivos que se acaban de citar. En ese mismo lugar se indica que todas las medidas adoptadas serán «conformes con los principios generales del derecho comunitario», citándose expresamente el art. 6, apartados 1 y 2, del Tratado de la Unión Europea (que remiten a la Carta de Derechos Fundamentales de la Unión Europea y al Convenio Europeo para la Protección de los derechos Humanos y de las Libertades Fundamentales)[19].

Como se ve, la Directiva de 2002 fija una serie de condiciones para la actuación de los Estados en este campo. Hay que subrayar la idea de que las medidas que se tomen deben ser necesarias, apropiadas y proporcionadas en una sociedad democrática para fines específicos de orden público. Ello hace recordar la previsión del art. 8 del Convenio Europeo de 1950, donde las injerencias en la vida privada solo son posibles si se trata de medidas necesarias en una sociedad democrática, entre otras cosas, para la seguridad pública, la prevención de delitos o la protección de derechos.

Sobre esta base se dictó la 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[20]. Sería el tercer nivel de regulación que señalábamos *supra*, ahora ya declarado inválido, como veremos después. Su aprobación, controvertida

[19] El citado Reglamento (UE) 2016/679 no impone obligaciones adicionales a las establecidas en esta Directiva 2002/58/CE (art. 95). De todos modos, esta Directiva de 2002 tendrá que modificarse para adecuarla al Reglamento de 2016. Así también lo afirma el considerando 173 de dicho Reglamento.

[20] Sobre su génesis, *vid.,* en castellano, Vilasau (2006: 1 y ss.).

desde el primer momento, se vio impulsada por los atentados de Madrid en 2004 y de Londres en 2005[21]. En los considerandos de esta directiva se entendía que los objetivos de seguridad que se persiguen con la conservación «no pueden ser alcanzados de manera suficiente por los Estados miembros». En cambio, pueden lograrse mejor en el ámbito comunitario (considerando 21), por lo que procedía a armonizar las disposiciones estatales que obligan a los proveedores de servicios a la conservación de determinados datos generados o tratados por los mismos (art. 1.1 de la Directiva 2006/24/CE). Así las cosas, la directiva 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 el usuario registrado» (art. 1.2). No se aplica al contenido de las comunicaciones electrónicas (art. 1.2). La obligación de conservar datos también se extendía a los que dimanan de una llamada telefónica infructuosa (art. 3). Los datos conservados se proporcionarían a las autoridades nacionales competentes de conformidad con la legislación nacional, cumpliendo los requisitos de necesidad y proporcionalidad (art. 4). En el art. 5 se establecía un amplio elenco de categorías de datos que deben conservarse (datos para rastrear e identificar el origen de una comunicación; para identificar el destino de una comunicación; para identificarla fecha, hora y duración de la misma; su tipo; el equipo de comunicación del usuario; y para localizar el equipo de comunicación móvil). Se decía expresamente que «no podrá conservarse ningún dato que revele el contenido de la comunicación» (art. 5.2). Una previsión relevante era la que establecía el período de conservación, que se fijaba entre seis meses y dos años a partir de la fecha de la comunicación (art. 6). También se indicaba que los Estados miembros nombrarían a las autoridades públicas responsables de control de este proceso en sus respectivos territorios, que deberían ser independientes (art. 9). Otras previsiones se referían a la protección y seguridad de los datos y a los requisitos de almacenamiento de los datos conservados. Por lo tanto, la Di-

[21] Son diversos los documentos europeos de naturaleza política que inciden en la importancia de los datos de comunicaciones para enfrentarse a la inseguridad. En este sentido, la Declaración del Consejo de Europa para combatir el terrorismo, de marzo de 2004, apunta la necesidad de una norma que regule la retención de datos; y la Declaración del Consejo de Ministros de la Unión Europea, de 31 de julio de 2005, recoge como objetivo que se elabore una norma sobre retención de datos para octubre de dicho año. En cambio, en esa época, el supervisor europeo de Protección de Datos no estaba convencido de la necesidad de la retención de datos (Dictamen de 26 de septiembre de 2005: disponible en: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2005/05-09-26_data_retention_ES.pdf).

rectiva de 2006 suponía una excepción al régimen general de protección de la vida privada contemplado en las Directivas 95/46 y 2002/58.

Esta Directiva de 2006 fue criticada desde el primer momento. Tal vez se equivocó el legislador comunitario al optar por un instrumento armonizador como la directiva, conformada desde la libre circulación de servicios, que poco tiene que ver con el Tercer Pilar, el Espacio de Libertad, Seguridad y Justicia, desde donde seguramente se hubiera actuado con un mayor *garantismo.* Ello quizá explique que la transposición de esta Directiva no se haya hecho de manera uniforme[22], lo que, por cierto, era una recomendación del Grupo[23] del art. 29 en su Dictamen 3/2006. La autorizada voz de Rodotá ejemplifica este ambiente crítico al indicar que la Directiva suponía «convertir de entrada a los ciudadanos en sospechosos y entrar en un nuevo marco donde se produce un fichaje masivo de datos»[24]. El 8 de abril de 2011 la Comisión Europea publicó un informe de evaluación de la aplicación de la susodicha directiva en el que, por un lado, concluía que la conservación de datos ha demostrado utilidad en

[22] La mayoría de los países optaron como finalidad de la retención la investigación de delitos (Dinamarca, Grecia, Chipre, Italia, Portugal, Malta). Sin embargo, otros no responden a eso: en Bélgica también se prevé ante el uso abusivo de las comunicaciones electrónicas; en Francia, la protección de la propiedad intelectual; en Eslovenia, la protección de los intereses económicos del país; incluso a veces se alude a investigación de delitos de pena de cárcel superior a un año (Luxemburgo), tres (Estonia), o cinco (Irlanda). Los destinatarios de los datos también varían. Respecto al período de conservación, hay casos tanto de seis meses (Chipre, Lituania, Luxemburgo), como de un año (Dinamarca, Estonia, Holanda, Portugal, Francia, Reino Unido) y de dos (Polonia, Italia —llamadas de teléfono—, Irlanda —también llamadas de teléfono—). En Suecia se entendió que no era necesaria la transposición. En Alemania, República Checa y Rumanía, sus tribunales constitucionales anularon las leyes nacionales aprobadas en la materia. En el país teutón por el «estado de vigilancia» del individuo que producía la retención; en Chequia se consideró que no existían garantías suficientes frente al posible abuso de los poderes públicos; y en Rumanía se criticó la ambigüedad del objeto de la ley. La República Checa y Rumanía aprobaron nuevas leyes sobre el particular.

[23] Se denomina así al Grupo de Protección de las Personas en lo que respecta al tratamiento de datos personales creado en virtud de lo previsto por el art. 29 de la Directiva 95/46/CE (cuando se aplique la nueva normativa europea —*vid.* nota 17— toda referencia a este Grupo se entenderá hecha al futuro Comité Europeo de Protección de Datos que crea el Reglamento de 2016). En dicho dictamen este Grupo de Trabajo recomendaba avanzar en las medidas de seguridad técnica y organizativa.

[24] Rodotá (2006: 53). La prevalencia de las lógicas de la reutilización y de la interconexión afectan a los principios esenciales de la protección de datos (*ibidem,* 55).

las investigaciones penales y, por otro, vertía críticas sobre el diseño de la directiva en lo referido al respeto de la intimidad[25]. Así las cosas, la Comisión manifestaba su intención de adoptar una reglamentación más estricta del almacenamiento de datos, el acceso a los mismos y su utilización.

También la industria arremetió contra esta normativa al considerar que tenía un impacto económico relevante o enorme para los proveedores de servicios pequeños. La Directiva no preveía el reembolso de los costes de los operadores que se ven impelidos a la conservación de datos.

Pues bien, como ya hemos avanzado, el TJUE, en una muy relevante decisión, declaró inválida la susodicha Directiva 2006/24/CE[26]. Es el Caso Digital Rights Ireland Ltd y Seitlinger y otros, Sentencia de 8 de abril de 2014[27]. Los asuntos acumulados que resuelve esta resolución tienen su origen en sendas peticiones de decisión prejudicial planteadas por la *High Court* de Irlanda y el *Verfassungsgerichtshof* austríaco, ambos críticos con la citada directiva.

En el argumentario del TJUE se echa en falta, tal vez, un uso más riguroso del principio de proporcionalidad, en sus diversos aspectos o escalones, aunque bien es cierto que la declaración de invalidez se funda claramente en la desproporción de la Directiva 2006/24/CE. El TJUE parte de que la conservación de metadatos afecta a la vida privada (art. 7 de la Carta de derechos Fundamentales de la Unión Europea), a la protección de datos (art. 8 de dicha Carta) y a la libertad de expresión (art. 11 de la Carta). A pesar de ello entiende que no se ha vulnerado el contenido esencial de estos derechos (apartados 38 a 40), y que hay un objetivo de interés general en la retención (apartados 41 a 45). El problema, en cambio, lo halla en la desproporcionalidad de la injerencia, lo que la hace injustificada[28]. Es decir, se considera que el legislador de la Unión Europea «sobrepasó los límites que exige el respeto del principio de proporcionalidad» en relación con los derechos implicados (apar-

---

25 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:es:PDF.

26 En esta decisión se ve una influencia de la jurisprudencia constitucional alemana, fijada sobre todo en la Sentencia de 2 de marzo de 2010 (1 BvR 256/08), que se encuentra en BVerfGE 125, 260.

27 En castellano esta sentencia puede consultarse en http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dde9be560acd034bd1a965e91d0b0aec4c.e34KaxiLc3qMb40Rch0SaxuQahj0?text=&docid=150642&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=220184.

28 Habida cuenta la relevancia de la injerencia en el respeto a la vida privada «la facultad de apreciación de legislador de la Unión resulta reducida, por lo que el control de dicha facultad debe ser estricto» (apartado 48).

tado 69). Esta desproporción se localiza en tres puntos: la Directiva 2006/24 «abarca de manera generalizada a todas las personas, medios de comunicación electrónica y datos relativos al tráfico sin que se establezca ninguna diferenciación, limitación o excepción en función del objetivo de lucha contra los delitos graves» (apartado 57 de la Sentencia); no se fija ningún criterio que delimite el acceso de las autoridades con base en delitos «suficientemente graves para justificar «la injerencia en los derechos fundamentales de los arts. 7 y 8 de la Carta» (apartado 60); y el período de conservación no contempla ninguna distinción entre las categorías de datos «en función de su posible utilidad para el objetivo perseguido o de las personas afectadas» (apartado 63). La injerencia en la protección de datos se entiende «de gran magnitud» y «especialmente grave» (apartados 37 y 65), «sin que esta injerencia esté regulada de manera precisa por disposiciones que permitan garantizar que se limita efectivamente a lo estrictamente necesario» (de nuevo el apartado 65). A mayor abundamiento el TJUE también considera que la directiva no contiene suficientes garantías «contra los riesgos de abuso y contra cualquier acceso y utilización ilícitos» de los datos (apartado 66). En fin, se censura igualmente que la directiva «no obliga a que los datos se conserven en el territorio de la Unión», por lo que no puede considerarse que el control de las medidas de seguridad esté garantizado por una autoridad independiente.

Tras esta Sentencia, la reflexión que surge es su alcance en el ámbito interno, o sea, en los ordenamientos de los Estados miembros. Desde un punto de vista formal, la anulación de una directiva no da lugar, a su vez, a la anulación de la norma interna que desarrollaba tal directiva. No existe ninguna relación de interdependencia. Sin embargo, desde una perspectiva de fondo, la legitimidad de la normativa interna que es una transposición de una directiva inválida puede quedar en entredicho. La respuesta *de lege ferenda* a esta situación operaría en ambos niveles: a nivel comunitario habrá que adoptar otra directiva[29], y en los Estados miembros es recomendable revisar las respectivas normativas si se entiende que no se adecúen al marco que ha fijado la sentencia de 2014. De todos modos, téngase en cuenta que la Directiva 2002/58/CE sigue en vigor, por lo que el derecho comunitario continúa posibilitando que

[29] La comisaria Cecilia Malmström, con oportunismo, se apuró a declarar, el mismo día en que está fechada la sentencia anulatoria, el 8 de abril de 2014, que esta decisión confirma las conclusiones críticas del informe de evaluación, ya citado, de la Comisión de 2011, y que la Comisión «proseguirá su trabajo en función de los avances realizados en la revisión de la Directiva sobre la intimidad de las comunicaciones electrónicas». Disponible en: http://ec.europa.eu/spain/pdf/ip090414-2.pdf.

se establezca un régimen excepcional de conservación de datos, a la que se pueden asir los Estados para su regulación.

Por lo tanto, la conclusión a día de hoy es que, pese a la invalidez de la Directiva de 2006, la pervivencia de las previsiones en la Directiva de 2002 (art. 15.1) permite emitir normas nacionales más rigurosas con el principio de proporcionalidad y necesidad que la anulada directiva de 2006. Sea como fuere, como indica Galán Muñoz analizando la política criminal de la Unión Europea, tras una fase inicial basada en el principio de disponibilidad, ha llegado una segunda en la que prima el rol a jugar por la garantía del respeto de los derechos fundamentales, gracias a la aprobación del Tratado de Lisboa y al impulso de la comentada sentencia del TJUE[30]. El regulador europeo se encuentra sometido a un verdadero reto reformador.

3. ESPAÑA

En nuestro país el legislador actuó con prontitud y ya en el art. 12 de la Ley 34/2002, de Servicios de Sociedad de la Información y Comunicaciones Electrónicas, estableció las bases de un sistema de conservación al referirse a la obligación de los prestadores de retener los datos de tráfico. Tal previsión no se materializó y el precepto fue derogado por la Ley 25/2007.

Así las cosas, hoy en día existe una regulación general y otra específica en el tema que nos concierne. La general se encuentra en la Ley 9/2014, de Telecomunicaciones, en cuyo art. 42 se prevé de una manera sucinta que la conservación y cesión de los datos generados o tratados en las comunicaciones «a los agentes facultados a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves» se rige por lo establecido en la Ley 25/2007.

Por su parte, la regulación específica la conforma esta Ley 25/2007, de 18 de octubre, de Conservación de Datos Relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones. Dicha Ley transpone la directiva anulada, la 2006/24/CE. La Ley 25/2007 impone a los operadores la obligación de conservación de los datos de tráfico, localización e identificación de usuarios, y regula la cesión de tales datos a las autoridades policiales, en el marco de una autorización judicial y para fines de detección, investigación y enjuiciamiento de delitos graves (art. 1.1). Los agentes facultados para recibir la cesión son los miembros de las fuerzas y cuerpos de seguridad, los funcionarios de la Dirección Adjunta de Vigilancia Aduanera y el personal del Centro Nacional de Inteligencia (CNI) (art. 6.2). Los dos primeros cuando

30 Galán Muñoz (2014: 10).

desempeñen funciones de policía judicial; los miembros del CNI en el curso de sus investigaciones «sobre personas o entidades». Los usuarios afectados son tanto personas físicas como jurídicas (art. 1.2). Sea como fuere, la conservación excluye el contenido de la comunicación (arts. 1.3 y 3.2). Los datos objeto de conservación que enumera la Ley reproducen lo previsto en la directiva anulada: datos necesarios para rastrear e identificar el origen y el destino de la comunicación, determinar su fecha, hora y duración, identificar el tipo de comunicación y el equipo utilizado, y la localización cuando se usen equipos móviles (art. 3). También se conservan los datos relativos a las llamadas telefónicas infructuosas (art. 4.2)[31], pero no los que se refieren a las llamadas no conectadas (art. 4.3)[32]. La conservación prevista es de doce meses, aunque se establece que reglamentariamente se podrá ampliar o reducir tal plazo en el margen que señalaba la directiva, o sea, de seis meses a dos años (art. 5.1). Para esta decisión se considerará el coste del almacenamiento y la conservación de los datos, y el interés de estos para la investigación de delitos graves. La resolución juridicial que autoriza la cesión fija el plazo de ejecución para dicha orden de cesión (art. 7.3). De no establecerse un plazo concreto, la ley prevé supletoriamente el de setenta y dos horas contadas a partir de las ocho horas del día laborable siguiente en que el operador reciba la orden. También se alude a la necesidad y proporcionalidad para elaborar esta resolución judicial (art. 7.2).

Asimismo, se establecen que los sujetos obligados «adoptarán las medidas necesarias para garantizar» una correcta conservación (art. 4.1). Así, los operadores deben impedir el uso de los datos para fines diferentes a los establecidos en la ley, la destrucción o pérdida de tales datos o su tratamiento o divulgación no autorizados (art. 8.l). Y todo ello, de conformidad, como no podía ser de otro modo, con la normativa de protección de datos (art. 8.l). En este sentido, el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos (Real Decreto 1720/2007), en lo relativo a las medidas de seguridad, ha asignado las de nivel medio para los ficheros de datos de tráfico y de localización, a la que se añade la medida de seguridad alta prevista para el registro de accesos (art. 81.4). El incumplimiento de estas obligaciones da lugar a la apli-

[31] Una llamada infructuosa, en términos de la propia ley, es «aquella comunicación en el transcurso de la cual se ha realizado con éxito una llamada telefónica pero sin contestación, o en la que ha habido una intervención por parte del operador u operadores involucrados en la llamada».

[32] La llamada no conectada, de nuevo citamos a la ley, es «aquella comunicación en el transcurso de la cual se ha realizado sin éxito una llamada telefónica, sin que haya habido intervención del operador y operadores involucrados».

cación de las sanciones administrativas propias de las telecomunicaciones, las relacionadas con las infracciones en materia de protección de datos, y las penales correspondientes. Esta coexistencia de regímenes sancionadores puede originar problemas, sobre todo en el ámbito administrativo.

La doctrina ha defendido la validez de nuestra ley, al entender que se haya alejada de las críticas que el TJUE esgrimió contra la Directiva de 2006[33]. Incluso se defiende que la actuación de nuestros jueces en el control de la injerencia «podría suplir determinados déficits de normatividad de la norma habilitante»[34], lo que precisamente, a nuestro entender, es un argumento para reclamar la mejora de la regulación.

Es cierto que la Ley española 25/2007 tiene más calidad que la comunitaria en cuanto a las garantías ante la injerencia. Así, se alude a delitos graves previstos en el Código Penal o en leyes penales especiales, lo que gana concreción frente a lo que disponía la Directiva (delitos graves tal y como se definen en la legislación nacional de los Estados miembros —art. 1.1 Directiva—). Ello requiere el correlato de una interpretación estricta del concepto de delito grave y una actuación judicial consciente de ello, lo que a veces no sucede. También la ley española establece un único plazo de un año de conservación, frente a la horquilla de la directiva (entre seis meses y dos años). Asimismo, ante a la indefinición de la directiva de la autoridad nacional legitimada para el acceso, la ley española se refiere a un concreto proceso de investigación criminal (art. 7) bajo la salvaguardia de una autoridad judicial, y se fijan los destinatarios. Esta autoridad judicial determina los datos que se cederán a los agentes facultados (art. 7.2)[35]. Aquí hay que tener en cuenta la normativa que regula la cesión de datos de las operadoras a los agentes, en la Orden PRE/199/2013, por la que se define el formato de entrega de los datos conservados por los operadores de servicios de comunicaciones electrónicas o de redes públicas de comunicaciones a los agentes facultados. También hay más concreción al referirse a las medidas de seguridad, sobre todo por las precisiones de la normativa de protección de datos que ya citamos.

Sin embargo, esta Ley 25/2007 presenta igual generalidad en la obligación de conservación que la directiva, que es universal. Y el plazo de un año

33 En este sentido podemos citar a Rodríguez Lainz (2014).

34 *Ibidem,* 9.

35 Debemos interpretar que este art. 7 exige en todo caso autorización judicial, superando las dudas que puede originar su primer párrafo (con una poco clara remisión: «sin perjuicio de la resolución judicial»). Sostiene la misma opinión José Antonio Martín Pallín: «El equilibrio entre la conservación de datos y el secreto de las comunicaciones: implicaciones en el proceso penal» (VV. AA., 2008: 161-162).

sigue pareciendo excesivo. Sea como fuere, nosotros entendemos, como vamos a mostrar a continuación, que pese a la mayor fortaleza de la ley española frente a la directiva, es conveniente la reforma normativa, por las exigencias de la posición y alcance de los derechos fundamentales en juego. Esta reforma tiene que producirse tanto en el ámbito de la intervención de comunicaciones como en el de la retención. La modificación de la Ley de Enjuiciamiento Criminal (LECrim) en el año 2015 avanzó en lo primero (aunque mantenemos críticas como vamos a ver *infra*), pero no en lo segundo (el nuevo art. 588 ter j de la LECrim simplemente afirma, en la línea de la Ley de 2007, que los datos conservados «solo podrán ser cedidos para su incorporación al proceso con autorización judicial», que también puede permitir la búsqueda entrecruzada o inteligente de datos).

V. LA CONVENIENTE REFORMA DEL RÉGIMEN JURÍDICO ACTUAL EN ESPAÑA

La jurisprudencia europea señalada puede servir de motor para la actualización y mejora de nuestra regulación. Incluso, por qué no, de pretexto para llevarla a cabo. La relevancia del tema creemos que así lo aconseja. La conexión con diversos derechos obliga a tener en cuenta distinta normativa, al menos tanto la general de intervención de comunicaciones como la especial de retención de metadatos. En términos globales, en España aún se constatan en la legislación positiva insuficiencias ante la realidad digital que nos rodea con una singular intensidad. La solución pasa —estimamos que ya necesariamente— por realizar las pertinentes reformas legislativas para superar un contexto de inseguridad jurídica ciertamente criticable. El tema de los datos de tráfico es un claro exponente de ello. Estas reformas permitirán avanzar, usando la terminología del TEDH, en la calidad de la ley, en su accesibilidad y previsibilidad, mejorando su consideración como una medida necesaria en una sociedad democrática (TEDH, caso Kopp contra Suiza, Sentencia del 25 de marzo de 1998, apartado 54).

Los comentarios sobre esta cuestión los dividimos en dos subapartados, pues, como vimos, la retención de metadatos también afecta al secreto de las comunicaciones, por lo que hay que tener en cuenta el régimen del mismo, extremo que parece no querer reconocerse todavía.

1. LA INTERVENCIÓN DE COMUNICACIONES

Respecto a la intervención de comunicaciones, *lege ferenda* estimamos que debería preverse un régimen general de intervención, donde también se

incluirían los datos de tráfico que hemos dicho que se integran en el contenido del derecho al secreto de las comunicaciones (identidad de los intervinientes). A partir de este régimen general se especificaría lo que fuera necesario para las distintas modalidades de comunicación. El régimen general tiene que fijarse en la LECrim.

Esta regulación debe poseer la calidad adecuada. Para ello la jurisprudencia ofreció pautas claras y precisas, que pueden guiar sin sobresaltos al legislador. Como es conocido, la regulación española en esta cuestión mostró carencias de magnitud. Así, el TEDH puso de manifiesto las deficiencias de la regulación española, tanto antes de la reforma de 1998 (el ya citado Caso Valenzuela Contreras) como después de esta (Caso Prado Bugallo *vs.* España, Sentencia del 18 de mayo del 2003, apartados 26 y ss.) al considerar que todavía era insuficiente la determinación de la naturaleza de las infracciones que pueden dar lugar a las intervenciones, la fijación de los límites temporales y de las condiciones de aportación de la prueba al juicio oral[36]. Ante estas carencias la jurisprudencia española, siguiendo al TJUE, señaló los requisitos necesarios para la intervención[37]. Además, se criticaron los déficits del antiguo art. 579 de la LECrim[38], que noso-

[36] En otras sentencias subraya la necesidad de que la interceptación esté prevista mediante ley, accesible al justiciable y predecible, y necesaria en una sociedad democrática (TEDH, entre otros, el ya citado Caso Kopp *vs.* Suiza y el Caso Messina *vs.* Italia, Sentencia de 28 de septiembre de 2000). La proporcionalidad resulta imprescindible (TEDH, Caso Foxley *vs.* Reino Unido, Sentencia de 20 de junio de 2000). Además, también ha precisado que el control puede producirse por parte del poder judicial en tres estadios: cuando se ordena la intervención, mientras se lleva a cabo o tras su finalización (TEDH, Caso Klass y otros *vs.* Alemania, Sentencia de 6 de septiembre de 1978). Referencias generales a las salvaguardas necesarias en la regulación se esquematizan en el Caso Kruslin *vs.* Francia, Sentencia de 24 de abril de 1990; y en el Caso Huvig *vs.* Francia, Sentencia de 24 de abril de 1990.

[37] Necesidad de motivación (STC 54/1996); la resolución judicial de autorización debe recoger tanto las razones fácticas como jurídicas que apoyan la necesidad de la intervención, el objeto de la medida tiene que precisarse con la mayor certeza posible, lo que se traduce en indicar el número de teléfono, las personas cuyas conversaciones han de ser intervenidas con determinación del grado de intervención, el tiempo de duración de la intervención, quiénes han de llevarla a cabo y cómo, y los períodos en los que debe darse cuenta al juez de los resultados para controlar su ejecución (STC 202/2001, STS de 16 de diciembre de 2002, ATS de18 de junio de 1992). La prórroga de la intervención también está sometida a motivación específica (SSTC 49/1999, 138/2001).

[38] En lo que se refería al plazo máximo de duración de las intervenciones, al control del resultado de las mismas y de los soportes en que consten, a las condiciones de incor-

tros en su día calificamos como un ejemplo de mala técnica legislativa[39]. Hemos denunciado que esta situación provoca un claro riesgo de inseguridad jurídica[40].

En esta línea, ha sido un avance la reforma de la LECrim operada por la Ley Orgánica 13/2015[41], si bien permanecen aspectos censurables. En efecto, entendemos que tras 2015 ha mejorado la regulación de la intervención de las comunicaciones en España (se ha ganado previsibilidad y certeza), pero esta reforma se ha quedado corta, lo que no deja de sorprendernos en una temática de esta envergadura. Propugnamos, por un lado, que se introduzca un régimen general de intervención de comunicaciones, que se completaría con ciertas especificaciones en función del soporte que se emplea para la comunicación (correspondencia escrita analógica, comunicaciones orales presenciales, teléfono, comunicaciones telemáticas como correo electrónico o chat cerrado, etc.). Las disposiciones generales previstas en los arts. 588 bis a) y siguientes de la LECrim no son un régimen general de intervención, aunque sean una base para establecerlo. Por otro lado, sugerimos que se establezca un régimen general para las medidas de investigación que afecten a la intimidad, que también tendría unas especificaciones adicionales (entrada y registro en lugar cerrado, registro de libros y papeles, dispositivos de seguimiento y localización, registro de equipos informáticos, captación de imágenes, etc.). Los datos de tráfico se verían regulados por ambos tipos de previsiones en función de si se integran o no en el secreto de comunicaciones, como ya vimos.

Sin duda, la reforma de 2015 es un esfuerzo de modernización del Título VIII del Libro II de la LECrim, para lo que cambia enunciados, reagrupa artículos, modifica capítulos e introduce otros nuevos. Se trata de dar cobertura legal a ciertas prácticas que existían en las investigaciones de una manera fáctica (y que la STC 145/2014 puso en duda, censurando la colocación de

---

poración a los atestados y al proceso de las conversaciones intervenidas (STC 184/2003). En esta sentencia se concluía que la situación no se ajustaba a las exigencias de previsibilidad y certeza en el ámbito de este derecho fundamental (FJ 7), por lo que instaba al legislador para que en el plazo más breve posible regulara con la suficiente precisión la materia.

39 Fernández Rodríguez (2004b: 117).

40 *Ibidem*, 139.

41 La reforma de 2015 de la LECrim partió de un proyecto de ley para la agilización de la justicia penal y el fortalecimiento de las garantías procesales, que se presentó en el Congreso de los Diputados el 13 de marzo de 2015. El Anteproyecto del Consejo de Ministros de 5 de diciembre de 2014 de reforma de la Ley de Enjuiciamiento Criminal se desgajó en dos proyectos de ley, uno de ley orgánica (el señalado) y otro de ley ordinaria (que afectó a cuestiones procesales como la agilización de la justicia penal).

micrófonos ocultos en centros de detención). Ello realmente es muy positivo. Pero se echa en falta, además de lo dicho en el párrafo anterior, una mejor sistemática (la numeración de los artículos es una complicación bien ilustrativa: ¡desde «bis» hasta «octies», desde «a» hasta «m»!) y un nuevo abordaje global del tema desde los postulados que ya están asentados.

2. LA NORMATIVA ESPECÍFICA SOBRE DATOS DE TRÁFICO

Dijimos antes que, aunque la vigente Ley española de Conservación de Datos de Tráfico muestra menos carencias que la Directiva 2006/24CE, esa Ley 25/2007 también presenta déficits que reclaman su reforma.

Resulta imprescindible que la regulación de la conservación de datos, como una limitación de un derecho, se haga por ley, que se ajuste al principio de proporcionalidad y que respete el contenido esencial de los derechos implicados. Así, la conservación debe respetar el contenido esencial de la protección de las comunicaciones no permitiendo entrar en el mensaje como tal. Este extremo sí está previsto.

En cambio, consideramos excesivo que se retengan de manera general los metadatos de todas las personas, independientemente de que existan o no indicios delictivos respecto de ellas[42]. Una vigilancia masiva y general es por sí misma sospechosa de desproporción, origina una percepción de control que obstaculiza el ejercicio de derechos. La conservación se extiende a todo el territorio y a todo el período temporal que se prevé. La aplicación general a todas las personas hace que la injerencia no resulte necesaria por su mismo exceso, ni mucho menos ponderada, con lo que se resienten dos de los subprincipios de la proporcionalidad, aunque quede cubierta la idea de adecuación a la finalidad perseguida (lucha contra el terrorismo y crimen organizado). Por lo tanto, no debería establecerse esta obligación universal de retención, de hecho sería preferible que se fijara un alcance menos general, como determinadas áreas geográficas, períodos de tiempo o grupo de personas[43]. También debería prohibirse la obtención de datos en ciertas comunicaciones, como las ligadas al secreto profesional o las basadas en una confidencialidad emocional.

Además, debería limitarse a los supuestos verdaderamente graves, esto es, limitar el alcance de la retención a delitos de terrorismo y delincuencia orga-

[42] Este carácter indiscriminado es el principal argumento que emplea la doctrina para objetar el sistema de retención de datos. Por ejemplo, González López (2006: 5-6).

[43] El Grupo del art. 29, en su Dictamen 9/2004, veía desproporcionado convertir lo que antes era la excepción en la regla general.

nizada[44]. La actual referencia a «delitos graves» es demasiado amplia e imprecisa. Incluso en un supuesto la ley española alude a delitos sin más: en el párrafo 4 de la Disposición Adicional única se establece la obligación de los operadores de ceder los datos identificativos de las tarjetas telefónicas de prepago a ciertas autoridades «con fines de investigación, detección y enjuiciamiento de un delito». En el Preámbulo de la Ley 25/2007 el legislador parece cometer un lapsus (¿revelador?) al indicar en su apartado II que la obligación de conservar los datos tiene como fin «la detección, investigación y enjuiciamiento de un delito». No se refiere a un delito grave, lo que abunda más en nuestra reflexión anterior de ser más preciso y exigente.

Respecto al rango normativo empleado, también vemos dudas. La Ley 25/2007 es una ley ordinaria que, como apunta Ortiz Pradillo, regula de una forma insuficiente la cesión de datos (art. 7.2) o excepciona la Ley Orgánica de Protección de Datos (art. 9)[45]. La LECrim, reformada por la citada LO 13/2015, ya alude a la intervención de datos de tráfico y a su incorporación al proceso. Pero ello no disipa lo apuntado sobre la Ley 25/2007.

Asimismo, señalamos otras carencias que necesitan mejora: el listado de datos lo vemos demasiado amplio y exhaustivo, es decir, excesivo, por lo que sería conveniente reducir las categorías de datos que deben conservarse[46]; no se precisa legalmente el procedimiento de acceso y sus condiciones (en el ámbito administrativo se regula el formato de entrega de los datos conservados, en la ya aludida Orden PRE/199/2013, lo que consideramos insuficiente); el período de retención de un año resulta demasiado largo, debería fijarse el de seis meses[47]. Tendrían que preverse en la normativa específica garantías de seguridad que protejan los datos conservados, más allá de la remisión a la legislación de protección de datos; en este sentido, deberían preverse medidas de seguridad específicas y diferentes para el almacenamiento de datos, para acceder a ellos y recuperarlos, y para su utilizarlos; de igual forma, faltan precisiones en la ley específica que garanticen la destrucción definitiva de los datos.

---

44 El Grupo del art. 29, en su Dictamen 4/2005, consideraba que el objetivo de la retención debería limitarse a la lucha contra el terrorismo y crimen organizado.

45 Ortiz Pradillo (2010: 5-6).

46 Además, hay algún dato al que los operadores obligados a la conservación no tienen acceso (como el correo electrónico por Internet o la telefonía por Internet —la denominada VoIP—).

47 El Grupo del art. 29, en su dictamen 9/2004, aludía a un estudio que evidenciaba que las compañías de telecomunicaciones no reciben peticiones que superen los seis meses. En el informe ya citado de la Comisión Europea de 18 de abril de 2011 (nota 25 de este trabajo) se refleja que casi el 90 % de los datos que se solicitan en los distintos países cuentan con una antigüedad de seis meses o menos (p. 17).

Además, los problemas para determinar los sujetos obligados a la conservación en determinadas circunstancias resulta un déficit adicional de esta regulación. La industria también hizo esta denuncia[48]. El art. 2 de la Ley 25/2007, al regular los sujetos obligados, remite a la antigua Ley General de Telecomunicaciones (la ya derogada 32/2003) para fijar quiénes son los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones. Se está pensando en los proveedores de acceso, pero no en los prestadores de servicios (como los cibercafés). De nuevo, hay que reclamar una reforma normativa que aporte una precisión que ahora no existe en los sujetos obligados.

Asimismo, también resultaría de interés que la Agencia Española de Protección de Datos efectuase cierta supervisión. Por ejemplo, se podría establecer la obligación de que los agentes facultados para recibir los metadatos evacuen anualmente un informe a esta agencia sobre ello. De este modo, la agencia podría efectuar una auditoría sobre el particular que conllevaría una beneficiosa publicidad para el conocimiento ciudadano y un incremento de la *accountability* del poder público.

VI. CONCLUSIONES

En un escenario como el actual, plagado de riesgos y amenazas tanto para la seguridad pública como para la mismísima seguridad nacional (o sea, del propio estado), resulta razonable permitir la retención de los datos de tráfico de comunicaciones, al igual que la intervención de las propias comunicaciones. No debemos perder una visión realista de esta cuestión.

Pero lo que también resulta innegable es que tales actuaciones tengan la suficiente cobertura jurídica para poder llevarse a cabo. Nos referimos a la previsión en una ley de calidad —desde el punto de vista democrático—, robusta, que garantice el contenido esencial de los derechos en juego y que se aplique cumpliendo el principio de proporcionalidad. Reclamar este rigor se justifica si pensamos que los datos de tráfico presentan singular transcendencia jurídica, pues afectan a la intimidad, a las comunicaciones, a la protección de datos de carácter personal, a la libertad de expresión (y participación), y a la libertad de circulación.

---

[48] Martín Pérez Sánchez: «Posición del sector de telecomunicaciones ante la nueva regulación de conservación de datos: retos y dudas», en VV. AA. (2008: 127 y ss.). Sobre el entendimiento de cuáles son los sujetos obligados, *vid.* Rodríguez Lainz (2008: 5).

Como ha quedado reflejado en los apartados anteriores, proponemos actualizar el régimen vigente en España para la intervención de las comunicaciones y el específico de la conservación de metadatos. Para lo primero se debería establecer una regulación general para tal intervención, completada con previsiones específicas para los distintos supuestos. Para lo segundo, hemos indicado un elevado número de sugerencias de reforma normativa. La tarea pendiente la creemos relevante y de fuerte densidad jurídica democrática. Por ello, el legislador la debería abordar con rigor y celeridad. La reforma de 2015 de la LECrim no ha sido suficiente en este sentido, aunque mejora la situación. Se ha perdido una excelente oportunidad para dar el salto definitivo de calidad que reclamaba esta materia.

La relación entre seguridad y derechos humanos se articula en torno a dos líneas, ya señaladas, una positiva y otra negativa. Las dos líneas son complementarias, en el sentido de que se aplican al mismo tiempo en una sociedad. Así las cosas, al mismo tiempo hay que establecer un nivel adecuado de seguridad para que se puedan aplicar los derechos, y que las limitaciones a estos por razones de seguridad sean razonables y proporcionadas en una sociedad democrática. Debemos huir de discursos polarizados, que enfaticen tan solo uno de los platos de esta singular balanza y optar por las soluciones equilibradas. La resolución de los conflictos que surjan debe realizase caso por caso, ponderando los intereses en juego. El reto es transcendente, pues se trata de ofrecer un adecuado equilibrio entre seguridad y libertad, el verdadero nudo gordiano del presente para los decisores públicos.

Además, hay que insistir en el estricto respeto de dos de las garantías actuales: que los datos conservados no revelen el contenido de la comunicación; que la cesión se refiera a una comunicación concreta existiendo una autorización judicial previa. Esta autorización tiene que precisar los datos que serán cedidos y el plazo de ejecución de la orden de cesión. No hay que olvidar que también es de aplicación la normativa de protección de datos, que es una garantía de los usuarios frente al tratamiento de sus datos por las operadoras, abocadas a garantizar la confidencialidad y la seguridad de los datos conservados.

En este sentido, es de una particular relevancia la actuación de los jueces y tribunales en la interpretación de las injerencias en los derechos fundamentales, tanto a la hora de precisar lo que es un delito grave como en el momento de no recabar datos que puedan ser excesivos (datos, por ejemplo, alejados en el tiempo del momento en que tuvo lugar el suceso investigado, independientemente de que la legislación fije el plazo de un año). La práctica ofrece casos censurables[49]. La medida que autoricen, motivadamente, debe ser necesaria,

[49] Sobre las discrepancias jurisprudenciales, *vid.* Galán Muñoz (2013: 50 y ss.).

útil y proporcional, debiendo solicitarse y acordarse por escrito, con identificación de los solicitantes y con fines penales en exclusiva.

En fin, la regulación de cuestiones tecnológicas exige tener en cuenta la rápida evolución que se produce en tal materia. Otro argumento más para que el legislador esté atento a mejorar y adaptar su obra a las nuevas circunstancias, antes de que el vertiginoso avance de la tecnovigilancia mengue la calidad de nuestro sistema de garantías y niegue la razonable expectativa de privacidad de la ciudadanía.

Bibliografía

Brandariz García, J. A. (2014). ¿Una teleología de la seguridad sin libertad? La difusión de las lógicas actuariales y gerenciales en las políticas punitivas. En Presno Linera, M. A. (coord.). *Fundamentos. La metamorfosis del estado y del derecho* (pp. 313-354).

Fernández Rodríguez, J. J. (2004a). *Lo público y lo privado en Internet. Intimidad y libertad de expresión en la Red*. México D.F.: Universidad Nacional Autónoma de México.

— (2004b). *Secreto e intervención de comunicaciones en Internet*. Madrid: Civitas.

— Jordán Enamorado, J. y Sansó-Rubert Pascual, D. (2008). *Seguridad y defensa hoy. Construyendo el futuro*. Madrid: Plaza y Valdés.

— (2012). La intervención de las comunicaciones digitales: a propósito del sistema SITEL. En J. J. Fernández Rodríguez, D. Sansó-Rubert Pascual, J. Pulido Grajera y R. Monsalve (coords.). *Cuestiones de inteligencia en la sociedad contemporánea* (pp. 61-75). Madrid: Ministerio de Defensa.

Galán Muñoz, A. (2013). ¿Nuevos riesgos, viejas respuestas? Estudio sobre la protección penal de los datos de carácter personal ante las nuevas tecnologías de la información y la comunicación. *Revista General de Derecho Penal* (19), 3.

— (2014). La protección de datos de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos: hacia una nueva orientación de la política criminal de la Unión Europea. *Diario La Ley*, 8356.

González López, J. J. (2006). La retención de datos de tráfico de las comunicaciones en la Unión Europea: una aproximación crítica. *Diario La Ley*, 6456.

López-Barajas Perea, I. (2011). *La intervención de las comunicaciones electrónicas*. Madrid: La Ley.

Ortiz Pradillo, J. C. (2010). Tecnología *versus* proporcionalidad en la investigación penal: la nulidad de la ley alemana de conservación de los datos de tráfico de las comunicaciones electrónicas. *La Ley Penal* (75), 5.

Pasolini, P. P. (1995). *Orgía.* Hondarribia: HIRUS.

Requejo Pajés, J. L. (1993). Constitución y remisión normativa. *Revista Española de Derecho Constitucional* (39), 115-160.

Rodotá, S. (2006). La conservación de los datos de tráfico en las comunicaciones electrónicas. *IDP. Revista de Internet, Derecho y Política*, 3, 53-60. Disponible en: http://www.uoc.edu/idp/3/dt/esp/rodota.pdf.

Rodríguez Lainz, J. L. (2003). *Intervención judicial en los datos de tráfico de las comunicaciones*. Barcelona: Bosch.

— (2008). El principio de proporcionalidad en la nueva ley de conservación de datos relativos a las comunicaciones. *Diario La Ley*, 6859.

— (2014). Sobre la incidencia de la declaración de invalidez de la Directiva 2006/24/CE en la ley española sobre conservación de datos relativos a las comunicaciones. *Diario La Ley*, 8308.

Rubio Llorente, F. (1993). *La forma del poder*. Madrid: Centro de Estudios Constitucionales.

Salamanca Aguado, E. (2014). El respeto a la vida privada y a la protección de datos personales en el contexto de la vigilancia masiva de las comunicaciones. *Revista del Instituto Español de Estudios Estratégicos* (4), 1-26.

Velasco Núñez, E. (2014). Tecnovigilancia, geolocalización y datos: aspectos procesales penales. *Diario La Ley*, 8338.

Vilasau, M. (2006). La Directiva 2006/24/CE sobre conservación de datos del tráfico en las comunicaciones electrónicas: seguridad v. privacidad. *IDP. Revista de Internet, Derecho y Política*, 3, 1-15. Disponible en: http://www.uoc.edu/idp/3/dt/esp/vilasau.pdf.

VV. AA. (2008). *La protección de datos en la cooperación policial y judicial*. Cizur Menor: Aranzadi.